BRIDGES AND LADDERS:

BUILDING THE LOGIC AND STRUCTURE FOR CYBERSPACE

BY

DAVID S. MILLER

A THESIS PRESENTED TO THE FACULTY OF

THE SCHOOL OF ADVANCED AIR AND SPACE STUDIES

FOR COMPLETION OF

GRADUATION REQUIREMENTS

SCHOOL OF ADVANCED AIR AND SPACE STUDIES

AIR UNIVERSITY

MAXWELL AIR FORCE BASE, ALABAMA

JUNE 2012

APPROVAL

The undersigned certify that this thesis meets masters-level standards of research, argumentation, and expression.

_____

COL MELVIN G. DEAILE (Date)

_____

DR. JOHN B. SHELDON (Date)

DISCLAIMER

The conclusions and opinions expressed in this document are those of the author. They do not reflect the official position of the US Government, Department of Defense, the United States Air Force, or Air University.

ABOUT THE AUTHOR

Major David S. Miller is a munitions maintenance officer with experience in conventional, nuclear, and ICBM maintenance. He received his commission in 1998 through the Reserve Officer Training Corps at the University of Nebraska – Lincoln, earning a bachelor's degree in Psychology. Major Miller completed intermediate level development education through the Air Force Intern Program, and earned a master's degree in Organizational Management at The George Washington University. While in the National Capital Region he worked in the Office of the Under Secretary of Defense for Policy and the Deputy Chief of Staff for Logistics, Installations and Missions Support.
Maj Miller has held a variety of positions within the wings in ACC, AFSPC, and PACAF. Prior to attending the School of Advanced Air and Space Studies, Major Miller commanded the 18th Munitions Squadron, Kadena Air Base, Okinawa, Japan. After school, he will join the J5 Directorate at United States Pacific Command, Camp H.M. Smith, Hawaii.

ACKNOWLEDGEMENTS

I would like to express my sincere appreciation to my thesis advisor, Col Melvin Deaile, for his guidance, wisdom, and support in exploring air, space, and mainly cyberspace. I would also like to thank my reader, Dr. John B. Sheldon, for lending his expertise, interest, and support of this excursion into cyberpower.

Special thanks to Maj Gen Brett Williams, Brig Gen Ken Wilsbach, Col Robert Morris, Col Michael Smith, Lt Col Jason Sutton, Lt Col Scott Brodeur, Maj Steve Anderson, Maj Adam Bixler, and Capt Clara Bayne for their thoughts and critiques as I wrestled with the ideas put forth in this thesis. The level of support I received during research trips, numerous phone calls, and discussions in the hallway cannot be overestimated. The brilliance within the people I have talked to greatly exceeds my ability to fully capture their assistance through this thesis. Therefore, the shortcomings and errors inside this paper are mine alone.

Most importantly, a heartfelt appreciation to the love of my life and our wonderful son. Their patience and understanding this year and throughout our entire career continues to inspire me. Thank you for your daily support, encouragement, and understanding. I would not be half the man I am, without the two of you. Yub Yub.

ABSTRACT

This thesis analyzes the organizational construct for command and control in cyberspace. Under the current model, USCYBERCOM utilizes a Centralized Control and Centralized Execution philosophy that runs counter to Air Force core tenants. The author illustrates how the air, space, and cyberspace domains are tied together to bridge the gap between United States' interests and enemies afar. Building on the interconnectedness of the three domains, the author provides an in-depth examination of how those domains utilize three different command and control models to leverage effects. The first chapter captures how the AOC controls flexible global power missions to deliver kinetic effects at subsonic speeds. The next chapter studies how the JSpOC controls the constellations of spaceborne satellites to deliver near real-time effects. The final case study illustrates how the USCYBERCOM command and control model defends and attacks from the GIG. By comparing and contrasting the three models, the author makes a recommendation for a hybrid model to command and control cyberspace. Only by authorizing the COCOMs to take some ownership of the cyber domain can they continue to develop the most effective and efficient strategies for their AORs, and to defend and attack at the speed of fiber optic light.

CONTENTS

ILLUSTRATIONS

Introduction

Figuring the Framework

If we have a thorough understanding of one system of relations […] we can use it to comprehend a system of relations we only begin to grasp, and, as a result, we get a feeling of security, well-being and power. Simply by naming features of a new experience, we fix and control that experience.

On July 4, 2009 the United States came under secret attack. Integral United States and South Korean websites helplessly collapsed under a barrage of "one and zeros" from North Korea or North Korean-sympathizers. A massive botnet attack flooded government and civilian sites with up to one million website hits per attack; 40 times as many users as the systems were able to support.[1] The "smoking gun" was a distributed denial of service weapon called the W32.Dozer virus. After infiltrating United States domains and crippling access to information, the malicious code began systematically targeting and deleting files with specific program roots.[2] Although the White House and Pentagon sites remained operational, the United States Treasury Department, Secret Service, Federal Trade Commission, and Transportation Department sites became casualties and shutdown for several days. Civilian targets included the financial district websites of the New York Stock Exchange, Nasdaq, and Yahoo Finance.[3]

---

[1] Associated Press and MSNBC, "US Eyes N. Korea for 'Massive' Cyber Attacks," updated July 9, 2009 (retrieved from http://www.msnbc.msn.com/id/31789294/ns/technology_and_science-security on December 29, 2011).
[2] Thomas Claburn, "Cyber Attack Code Starts Killing Infected PCs," *Information Week*, July 10, 2009 (retrieved from http://www.informationweek.com/news/government/security/218401559 on December 29, 2011).
[3] Choe Sang-Hun and John Markoff, "Cyberattacks Jam Government and Commercial Web Sites in US and South Korea," *New York Times*, July 9, 2009 (retrieved from http://www.nytimes.com/2009/07/09/technology/09cyber.html?adxnnl=1&pagewanted=print on December 29, 2011).

Fortunately, the attack was short-lived and the effects were mostly recoverable. Experts at Symantec Security estimated the cyber-attack fatalities were limited to a few thousand computers, and by triaging the disabled websites they were operational within a few days.[4] The unfortunate predicament is that the attack did not feel like an attack; at least not the type to which humans are accustomed. Fundamentally, the attack occurred without provocation or notice, and targeted American interests (rather than population). Albeit an electromagnetic assault resulting in access denial and information loss, the strikes did create hardware casualties and fatalities. One country attacked another and threatened its sovereign interests. Interestingly, the United States' response was to admonish the actors and took no known retaliatory actions. A problem with cyber war and cyber attack is that it is hard to determine the boundaries separating what constitutes war and how to respond to perceived attacks.

Reviewing the response (and assuming it did not lead to an in-kind attack or an escalation to the traditional forms of war), the nation's lack of retaliation to the attack spurs a number of questions. The military practitioner may ask, is the Department of Defense (DoD) susceptible to the same type of attack? How dependent is the military on the cyberspace domain? Is the United States organized and equipped to defend attacks on the military networks that occur with unprecedented speed? What does control mean in cyberspace and who should wield it? The pursuit of answers to those questions is the genesis for this thesis.

The DoD leverages an asymmetric advantage in the air, ground, sea, and space to fight for, secure, and protect America's interests. The geographic combatant commander's authorization to manage an area extends to the terrestrial domains but not the cyber domain. Today the cyber domain has the potential to share and affect the battlefield in ways

---

[4] Thomas Claburn, "Cyber Attack Code Starts Killing Infected PCs."

never before possible, and that impact is likely to grow. It is possible that planners and warfighters are disadvantaged and forced to accept unnecessary risks by not exerting operational control of the cyber domain. By studying the DoD's current model for cyberspace and comparing in to other command and control centers, conclusions and recommendations about the current model can be made. Only by using the right model can the DoD ensure its ability to defend and deter cyber-attacks in the future.

To begin the investigation, it is important to understand what the term cyberspace means. Current military doctrine and leadership statements are a source for comprehension. The following section will explore these sources and build a cyber-centric perspective for commonalities in the lexicon of command and control. The next step will be to build an understanding of what constitutes a domain and its utility in war. Only then can the framework of this thesis be used as a lens to study how the DoD operationalizes cyberspace, and contrast it against other environments. Evidence and recommendations can be drawn by studying how the DoD transforms air, space, and cyberspace into power. The desired goal is to ensure the DoD's command and control element fosters an environment that maximizes operating *in* and *through* cyberspace.

Assumptions and Definitions

All the expected documents and regulations to identify cyberspace as a domain currently exist. Joint Publication (JP) 1-02 and the DoD's 2010 Quadrennial Defense Review establish cyberspace as a ". . . a global domain within the information environment that encompasses the interdependent networks of information technology infrastructures, including the Internet and telecommunication networks[5] . . . cyberspace is now as relevant a domain for DoD activities as the naturally occurring

[5] Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, November 8, 2010 (updated October 15, 2011).

domains of land, sea, air, and space."[6] The DoD has five strategic initiatives that build a comprehensive Strategy for Operating in Cyberspace. The first of the initiatives is for the DoD to "treat cyberspace as an operational domain to organize, train, and equip so that the DoD can take full advantage of cyberspace's potential."[7] Air Force Doctrine Document (AFDD) 3-12 recognizes cyberspace as a domain no less than four times in the first two pages of the instruction.[8] Given the preponderance of evidence, cyberspace is clearly a domain, and one that the military uses to conduct operations *within* and enable operations *from* the electromagnetic spectrum.

Building on the DoD's recognition of cyberspace as a domain, there are critical questions left to be answered and require explanation to frame the remainder of the discourse. Understanding the concept of control and to what degree the United States can build an asymmetric advantage vary across the five domains: air, land, sea, space, and cyberspace. Likewise, the core tenets of centralized control and decentralized execution of operations varies across the domains.

The type of model used to command and control a domain speaks volumes about the importance of control, how the military governs that power, and how responsive the system is to requests for effects . This thesis will deconstruct three very different models that the United States Air Force (USAF) utilizes to conduct operations in air, space, and cyberspace, and make conclusions and recommendations about the current cyberspace model for command and control.

Constructing Control

Having a clear definition of war is the first step to understanding the integration of cyberspace with ground, sea, air, and space forces.

---

[6] Department of Defense Quadrennial Defense Review, February 2010, 37.
[7] Department of Defense Strategy for Operating in Cyberspace, July 2011, 5.
[8] AFDD 3-12, *Cyberspace Operations,* July 15 2010, 1-2.

Ironically, the DoD does not have a definition of war. It does, however, define conflict as "an armed struggle or clash between organized groups within a nation or between nations in order to achieve limited political or military objectives."[9] Military theorist Carl von Clausewitz, defined war as an ability to impose enough force to get the opposing belligerent to do one's will. He goes on to articulate the means of fighting as "physical force."[10] The Joint Staff and Clausewitz both posit that in war and conflict, the belligerents use a physical clash of force and violence to achieve their ends.

Collectively, JP 1-02 and *On War*, in their own different ways, shape how US military forces fight their wars to achieve desired political ends. Thus, the two documents together frame the definition of war. War is the political pursuit of national interests through the clashing of opposing armies, using physical force and violence. When reflecting on the opening anecdote about North Korea, questions arise as to what constitutes an attack and how cyberspace fits in a definition focused on physical force and violence.

Building on the definition of what war is, it is essential to analyze whether cyber is a new kind of war – in-and-of itself – or just a unique contribution to existing means of fighting in war. Although cyberspace introduces a unique ability to disrupt, what separates fighting in this newest domain is the *inability* to inflict physical force and violence. Even though cyberspace can enable and disrupt the physical effects waged from aircraft, tanks, and carriers, it has yet to actually inflict violence in the physical sense. Additionally, although humans pursue the ability to weaponize cyberspace, it will be a long time before the DoD is fighting wars wholly in that domain.

---

[9] Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*.
[10] Carl von Clausewitz, *On War* (Princeton, NJ: Princeton University Press, 1976), 75.

Currently, fighting from the cyber realm encompasses the ability to "add, alter, or falsify data, or cause the disruption of or damage to a computer, or network device, or the objects a computer system controls."[11] This certainly applies to the 2009 cyber-attack on the United States. Richard Clarke specifically stated cyber is "*not* some victimless, clean, new kind of war. . ."[12] His thoughts on whether cyber is a new type of war or merely a different means of fighting in a war are pertinent. Besides the obvious statement that cyber is not a new kind of war, he acknowledged that traditional war had victims and did not reside in a sterile, virtual battlefield. He asserted the important feature of violence. Violence is anything but clean, and victims of the violence occur on both sides.

From the above discussion, cyberspace has the ability to participate in a war but does not constitute a war unto itself. Therefore, cyberspace changes the character of war but not the nature of war. It is merely another medium to attack with and from. Cyber theorist Martin Libicki supports this assertion, "Warfare is the management of violence, not merely its generation."[13] He also proposes that cyber may someday become "the potential fulcrum" in fighting, but today it is merely one of many means of fighting in war.[14] Recognizing cyber's relation to war assists in understanding the DoD's interest in achieving a favorable amount of control and dominance in the domain.

David Lonsdale also illustrates this point when he writes, "information power still needs air, land or sea forces to destroy the targets it has identified, or to move supplies and troop deployments."[15]

---

[11] Richard Clarke & Robert K. Knake, *Cyber War: The Next Threat to National Security and What To Do* (New York, NY: Harper Collins Publishers, 2010), pg. 228.
[12] Richard Clarke & Robert K. Knake, *Cyber War*, pg. xiii.
[13] Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (New York, NY: Cambridge University Press, 2007), 95.
[14] Martin C. Libicki, *Conquest in Cyberspace*, pg. 161.
[15] David J. Lonsdale, *The Nature of War in the Information Age: Clausewitzian Future* (New York, NY: Frank Cass, 2004), 191.

Finally, when describing the inherent power of cyberspace, Franklin Kramer very carefully constructs a definition that bounds cyberspace's effects to creating advantages and influencing operations on the battlefield,[16] although its ability to attack the mind of the enemy is credible. In this respect, cyber is not the true "road to war," but a bridge to attack from and through, and a medium that allows forces to wage warfare.

Returning to the North Korean cyber attack , it lacked the violence and force of a physical clash between two militaries. Although it could have been an initiator for war, it did not rise to a level that precipitated posturing for physical conflict. This deduction supports the working definition of war, thereby supporting the proposal that cyberspace is a new domain for engaging in war, but is not ushering in a new era of warfare. Recognizing that the cyberspace domain is merely an enabler or contributor is important because it drives the discussion of who should wield its power. Before having that discussion, however, it is important to determine what control means in the virtual domain.

Antoine Bousquet articulates a historical perspective on the origin of command and control in his book *The Scientific Way of War*. Command represented the authority to disseminate orders for execution when early warfare did not possess the technologies to allow continuous feedback. The term control was added later when commanders were able to gain a feedback mechanism, granting them the ability to "exert continuous direction."[17] An interesting aspect of control is the concept of span of control, and it is helpful to look at early theorists' views of other vast domains.

---

[16] Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem" in Franklin D. Kramer, Stuart H. Staff & Larry K. Wentz, *Cyberpower and National Security* (Dulles, VA: NDU Press and Potomac Books, 2009), pg. xvi.

[17] Antoine Bousquet, *The Scientific Way of Warfare: Order and Chaos on Battlefields of Modernity* (New York, NY: Columbia University Press, 2009), 128-129.

Julian Corbett's thoughts on control of the sea are very pertinent to conceptualizing control of the cyber domain. Corbett asserted the enormity of the sea prevented any single country from attaining complete supremacy of all the waters. He viewed control as existing in various degrees.[18] First, that control occurs locally. Second, that control occurs temporarily. Control is only attained through the lack of engagement from a belligerent or through winning a decisive victory, but in such situations the control is limited to that particular time and location. Control gained uncontestably or through a victory, is only held for as long as the victor remains in that place (locally) and for as long as the belligerent does not contest it (temporarily). The ultimate goal is to ensure the "enemy can no longer attack our lines . . . and that he cannot use or defend his own."[19]

AFDD 3-12 has a similar view of control in cyberspace. It refers to cyber superiority as being "localized in time and space."[20] The desire is to gain and maintain a status of supremacy, but much like Corbett's views of the sea, is not achievable or feasible. Subjecting the sea – just like cyberspace – to absolute control is not predisposed to traditional concepts of ownership. A ship cannot own the water or its position in the body of water. The best the ship can do is command a location for as long as the ship remains there, and is able to win any attempts to contest the control.

The idea of physically possessing a domain or even part of a domain translates even more poorly into cyberspace. It is possible to own a piece of electronic hardware and exercise possession of it, but cyberspace exists through the electronic impulses that flow within the hardware and all the rest of the hardware connected to the domain. The electromagnetic spectrum may control the size of the cyber domain in

---

[18] Julian Corbett, *Classics of Sea Power* (Annapolis, MD: Naval Institute Press, 1988), 102.
[19] Julian Corbett, *Classics of Sea Power*, 105 & 186.
[20] AFDD 3-12, *Cyberspace Operations*, 2.

some respects, but in others it is not confined or controllable due to the way the domain maps and connects users together.

When considering how to exert control over the cyber domain, Lonsdale's thoughts on the infosphere are germane. Like Corbett, Lonsdale asserted much of the domain was uncommanded.[21] In its everyday state, no nation-state controls cyberspace; it merely exists. Firewalls and passwords influence and control parts of cyberspace, as much as military and law enforcement agencies control sea lanes and airspace. Also like Corbett, Lonsdale believed one could achieve localized and temporary control. Similarly, Daniel Keuhl spoke of maintaining superiority in cyberspace: "the degree to which one can gain advantage from the use of cyberspace while if necessary preventing one's adversaries from gaining advantage from it."[22] Keuhl did not suggest maintaining absolute dominance or total control of the entire cyber domain, but rather maintain the ability to operate uncontested and deny the enemy from doing the same.[23] In cyberspace, like the sea, absolute control is unattainable.

Constructing a Cyber Bridge

Whether in sea, air, space, or cyberspace, commanders exercise localized and temporary control of the domains. Using the analogy of a suspension bridge, the tower of the bridge represents the commander and each cable represents the commander's ability to provide control in a specific location (Figure 1). Collectively, the suspension cables connecting the tower to the deck, represent the span of control. This allows for the weight of the bridge to be distributed. The effectiveness of the cables are localized and work as a part of a larger system. They are also temporary in that if anything happens to any one cable it changes

---

[21] David J. Lonsdale, *The Nature of War in the Information Age*, 185.
[22] Daniel T. Keuhl, "From Cyberspace to Cyberpower" in *Cyberpower and National Security*, 37.
[23] In instances it may be advantageous to allow the enemy to continue operating as it introduces the opportunity to gather intelligence, monitor actions, and alter, add, or disrupt information.

the forces and pressures on the ones around it. Symbolizing the tower, commanders are able to exercise their span of control in cyberspace. Just like the cables of the bridge, if the effectiveness of one of the cables is disrupted it creates stressors on the surrounding cables.

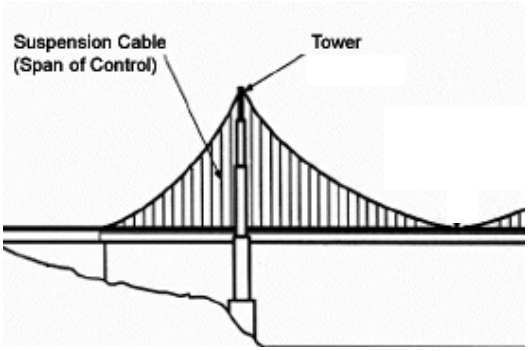

Figure 1: Suspension Bridge Diagram
Source: Adapted from
http://mmem.spschools.org/grade3science/3.bldg/Suspension.html

Understanding that cyberpower is a means of fighting in war and that asserting complete control cannot exist in cyberspace, integral issues about command and control of cyberspace, and whether that control should be centralized or decentralized, surfaces. These two points speak to the heart of this thesis, and requires a quick review of the Air Force tenets "Centralized Control" and "Decentralized Execution."

Joint Publication review of centralized control insinuates the concept is foreign to all domains except air. The terminology only exists in one document and within it states, "in joint air operations, placing within one commander the responsibility and authority for planning, directing, and coordinating a military operation or group/category of operations."[24] To the Air Force, centralized control is a fundamental principle in doctrine and prerequisite to ensuring proper apportionment, allocation, and leveraging of resources.[25]

Dispersed control and piecemeal dilution of air forces can lead to disastrous events. Quoting Air Marshall Sir Arthur W. Tedder, RAF, ". . .

[24] JP 3-30, *Command and Control of Joint Air Operations*, January 12, 2010, I-3.
[25] AFDD 6-0, *Command and Control,* June 1, 2007 (incorporating Change 1, July 28, 2011), vii.

if your organization is such that your air power is divided up into separate packets and there is no overall unity of command at the top, once again you will lose your powers . . . Air power in penny packets is worse than useless. It fritters away and achieves nothing."[26] The lesson learned from the World War Two battles in Africa preordained today's model for centralized planning and control, and decentralized execution. The battle over the Kasserine Pass of North Africa in 1942-43 is the "only important battle fought by the Armed Forces – either in World War II or since that time – without enjoying air superiority."[27] During Operation Torch the army divided the air forces into "multiple organizations with separate chains of command"[28] and aircraft were further broken into small "penny packets."[29] The role of the aircraft was to provide a flying artillery capability for the ground forces and consequently the Allies continually lost the air superiority battle. The inappropriate apportionment to a level below their ability to win contested aerial campaign led to losses on the ground as well as in the air.[30]

Given that airpower has redefined the speed and range of attack, and given the lessons learned in the Kasserine Pass battle, the conclusion was made to centralize the planning and coordination efforts to better support the commander's intent. Interestingly, the characteristics of speed and range require decentralized execution. The size, complexity, volume of operations, and speed at which the battlefield moves makes it unrealistic for a single commander to constantly manage a war. Not only would the diligence and complexity exhaust the

---

[26] Sir Arthur W. Tedder, "Air, Land, and Sea Warfare" as quoted by Lt Col Clint Hinote, "Centralized Control and Decentralized Execution: A Catch Phrase in Crisis?" *Air Force Institute Papers*, 2009-1, 9.
[27] Shawn P. Rife, "Kasserine Pass and the Proper Application of Airpower," *Joint Forces Quarterly*, Autumn/Winter 1998-1999, 71.
[28] Lt Col Clint Hinote, "Centralized Control and Decentralized Execution," 7.
[29] Ben Zweibelson, "Penny Packets Revisited: How the USAF Should Adapt to 21st Century Irregular Warfare," *Small Wars Journal*, September 29, 2010, 1. The author makes reference to how aircraft were misused by apportioning the aircraft to such a small level they could not mass effects.
[30] Shawn P. Rife, "Kasserine Pass and the Proper Application of Airpower," 72 & 76-77.

leadership, centralized execution would over-tax the system and retard battlefield flexibility and reaction to changing conditions. The key to operational success is building a framework to balance the appropriate amount of control and execution within a command and control structure.

Methodology

Fitted with a definition of war, cyberspace's relationship to war, an understanding of command and control, and the importance of centralized control and decentralized execution, the study of different models of command and control can begin. The next three chapters will take a critical look at the organizational structures, command and control processes, and models to wield power.

Chapter 1 will analyze the current Air Operations Center (AOC) construct and how the warfighter leverages airpower. Viewed as a weapon system, the AOC is the Air Force's solution for bringing coordinated airpower effects to the battlefield. As the command and control authority for aircraft in the Area of Responsibility (AOR), the chapter highlights extreme situations where aircraft begin and end their sorties in one AOR, while executing their missions in another. The study highlights shared responsibility for the welfare of the crew, the ability to bring effects to the battlefield, and the execution of long-range, slowly developing and continually evolving, subsonic missions.

The next chapter transitions from the AOC structure to a model developed for the integration of space assets. Chapter 2 uncovers how the Joint Space Operations Center (JSpOC) exploits the country's superiority of space to enable the warfighter. Further, it depicts how the JSpOC and AOC match – and ideally maximize – the capabilities of a small but continuous constellation with a voracious appetite for satellite products, to fight and win America's wars. Again, the command and control model for the organizational structure and its ability to employ national assets to produce near real-time effects is the focus.

The third chapter builds on the natural progression from airpower and space assets to an understanding of what cyberspace brings to the fight. Chapter 3 introduces cyberspace's integration into peace and wartime operations, effects leveraged by cyberspace, and its current model for delivering effects. Specifically, the chapter chronicles an examination of the United States Cyber Command (USCYBERCOM) organization and how it delivers capabilities and effects to the warfighters.

The final body of work, Chapter 4, compares and contrasts the three command and control models for air, space, and cyberspace. The analysis is an analytical comparison of how command and control continually shapes the battlefield; from manned flight to space exploration to cyberspace innovation. Common characteristics across the first three chapters include: small, finite numbers of platforms and limited inventory; adeptness to navigate and attack anywhere on the globe; ability to change the operational picture with the right configuration of weapons and targets; virtually undetectable weapons; and the difficulty of forensically attributing effects.

The chapter also contributes recommendations on the best way to exploit the use of cyberspace technologies. The focus aims at how Combatant Commanders (COCOMs) can best integrate cyberspace into their fighting forces. The danger in this approach, and the impetus for this thesis, is to determine whether cyberspace is *so different* that it warrants a completely different structure.

Chapter 1

AOC and the Air Domain

Airpower has become predominant, both as a deterrent to war, and – in the eventuality of war – as the devastating force to destroy an enemy's potential and fatally undermine his will to wage war.

-- General Omar Bradley

The previous chapter included an analogy relating parts of a bridge to the warfighter's span of control. To fully understand the analogy, it is helpful to take a couple of steps back and start at the beginning of the bridge construction. First, there exists a chasm. On one side of the gap, is the United States' political will and military power. On the other side, is the belligerent or crisis. The military instruments represent the coercive power or capability of the United States to bridge the chasm like an intercontinental roadway. The number of lanes in the road represents the amount of power or military services brought to bear. The AOC oversees the Air Force's lane of the road and the synchronization of air, space, and cyberspace effects.

The Air Force tenet of air superiority predicates the importance of establishing control of the skies at the onset of any conflict. Gaining uncontested control of the air allows for freedom to attack and maneuver. Conversely, without air superiority the risk to friendly forces in the air, sea, and ground domains greatly increases.[1] The AOC is constructed on the core Air Force tenets of "centralized planning and control, and decentralized execution."[2] This chapter will examine the organizational structure of the AOC. Studying the command and control relationships, means of requesting and delivering effects, and the battle

---

[1] AFDD 2, *Operations and Organization,* xii.

[2] AFI 13-1AOC, Volume 3, *Operational Procedures – Air and Space Operations Center,* November 2, 2011 (retrieved from http://www.e-publishing.af.mil), 5.

rhythm of operations will allow an analysis for the effectiveness of the model in air operations. Later, the AOC will be contrasted with other models to see if portions of the AOC structure are applicable to controlling cyberspace operations.

Aircraft belonging *to* and operating *from* one AOR, but striking targets *in another* AOR exemplifies the Air Force's global strike capability. It also codifies one of the more complex operations for the AOC. The culmination of this chapter captures the employment of the B-2 Stealth Bomber in Operation Allied Force. The weapon system offers to show how the command and control model of the AOC fits the delivery of munitions from a subsonic asset with global reach.

The Air and Space Operations Center

The genesis behind the AOC was the requirement to provide operational-level command and control of air and space forces. Within the published guidelines of the Joint Forces Commander[3] (JFC), the AOC becomes the AOR's nerve center and pivot point for planning and executing air and space campaigns. Following Air Force doctrine and bedrock principles involving unity of command, the AOC allows for all air and space assets to fall under the control of a single Airman.[4] Through the direction of this single Airman, the AOC directs and supervises "the activities of assigned and attached forces and to monitor the actions of both enemy and friendly forces."[5] Air and space operations accomplish command and control through strategy and planning development. In this way, the AOC governs which aircraft travel across the bridge and when they can move. The AOC organizes air activity to maximize effects and attain superiority in the air domain.

---

[3] The term Joint Forces Commander (JFC) is used to represent the command authority for a military situation. In a larger situation or in an AOR-wide operation the JFC could be the geographical combatant commander.

[4] AFDD 6-0, *Command and Control,* June 1, 2001 incorporating Change 1, July 28, 2011 (retrieved from www.e-publishing.af.mil), vii.

[5] AFTTP 3-3.AOC, *Operational Employment – Air and Space Operations Center*, November 1, 2007, 1-1.

The AOC functions as an all-inclusive communications suite that enables centralized planning and real-time synchronization of air, space, and cyber assets from multiple services and countries. A Joint Forces Air Component Commander (JFACC) provides leadership and direction for the AOC, as well as the air forces in the theater. Through the AOC, the JFACC is able to integrate manned and unmanned aircraft along with space-based systems for extensive awareness and flexibility to shape the battlefield. The JFACC relies on an AOC Commander to effectively manage air and space operations, and establish a battle rhythm.[6] The AOC is comprised of five divisions of diversely qualified career field experts (Figure 2).

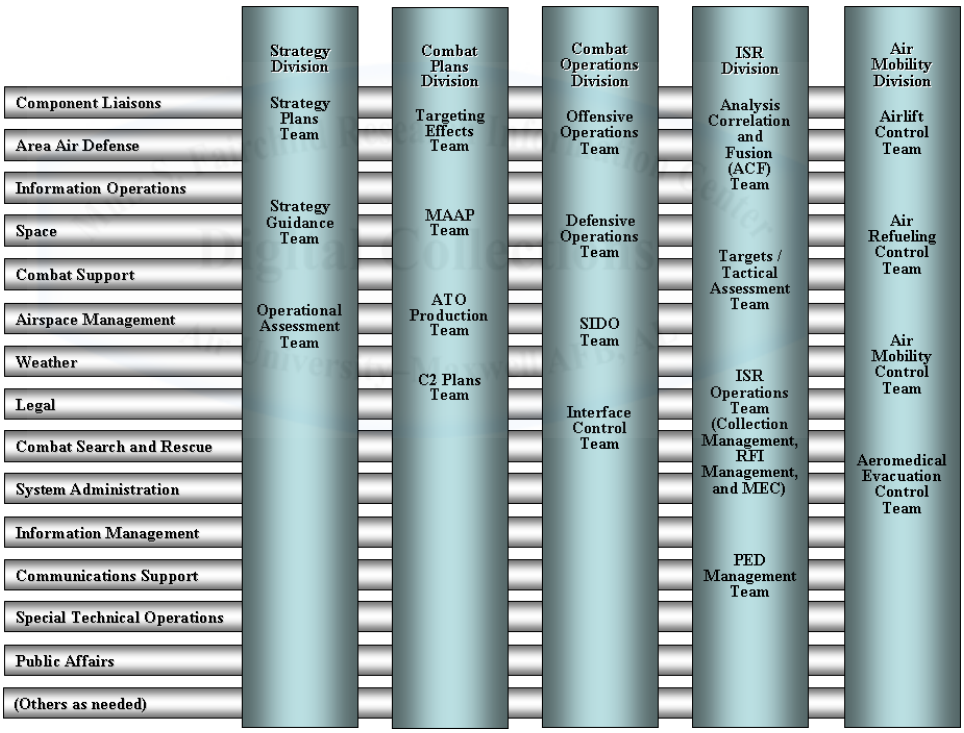

Figure 2: Basic Structure of the AOC
Source: AFTTP 3-3.AOC, Operational Employment – Air and Space Operations Center, November 1, 2007

The AOC establishes airpower guidance through an Air Operations Directive (AOD) and employs airpower through a daily Air Tasking Order

[6] AFTTP 3-3.AOC, *Operational Employment – Air and Space Operations Center*, 1-4.

(ATO). The AOD is similar to the commander's intent and represents the "air and space component's operational-level guidance" in supporting the JFC's overall objectives.[7] It is near-term strategy guidance, used to guide the creation and execution of the ATO.[8] The ATO takes the leadership's intent and assigns targets and combat air patrols. The objective is to allocate aircraft and weapons to targets to achieve desired effects in every 24 hour period.

The three offices most closely tied to the ATO are the Combat Plans Division (CPD), Combat Operations Division (COD), and Liaison Officers (LNOs). Behind the scenes a lot of work occurs that builds up to the ATO production, but the coalescing occurs in the CPD offices (Figure 3). They are responsible for near-term air and space operations.[9] The

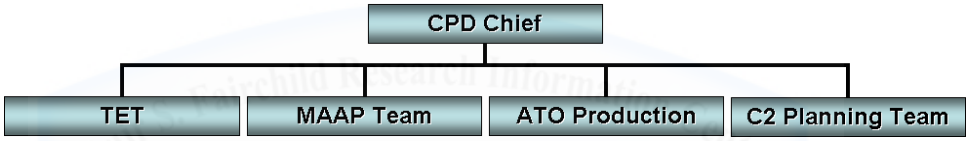

Figure 3: Combat Plans Division (CPD) Organization
Source: AFTTP 3-3.AOC, Operational Employment – Air and Space Operations Center, November 1, 2007

Master Air Attack Planning Team (MAAP), an office within the Combat Plans Division, reviews the AOD for JFC-guidance and assigns aircraft and munitions to missions and targets. The MAAP is comprised of subject-matter experts with knowledge and experience across a myriad of mission sets and aircraft.[10] Although the MAAP spans a breadth of skill-sets, it is not inclusive and often requires the advice of LNOs.[11] Only after interpreting the JFC-guidance, reviewing the list of available assets, and discussing the missions with the LNOs is the MAAP cell able to build and distribute the ATO.

---

[7] AFDD 2, *Operations and Organization*, April 3, 2007, 108.
[8] AFTTP 3-3.AOC, *Operational Employment – Air and Space Operations Center*, 3-46 & 3-51.
[9] AFTTP 3-3.AOC, *Operational Employment – Air and Space Operations Center*, 1-5 & 4-1.
[10] AFTTP 3-3.AOC, *Operational Employment – Air and Space Operations Center*, 4-28.
[11] AFTTP 3-3.AOC, *Operational Employment – Air and Space Operations Center*, 4-43.

After developing the ATO, the JFACC executes all air operations for the ATO cycle through the COD (Figure 4). The COD's existence revolves around executing the ATO, which is a plan, and Helmuth von Moltke reminds, ". . . no plan of operations extends with any certainty beyond the first contact . . ."[12]

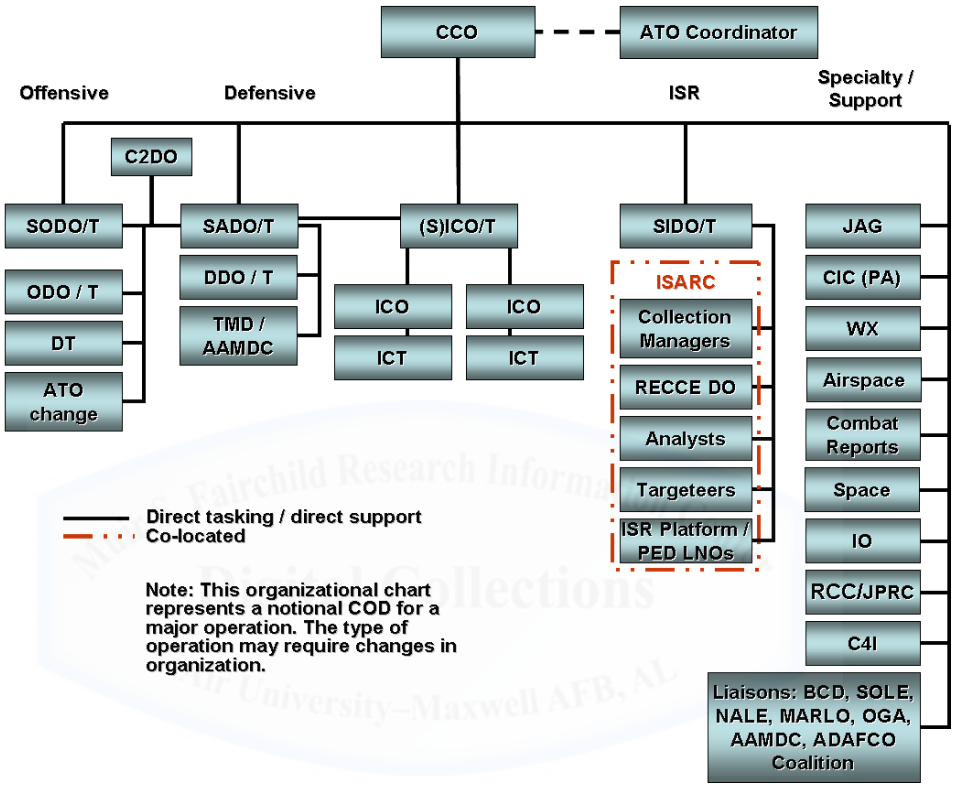

Figure 4: Combat Operations Division (COD) Organization
Source: AFTTP 3-3.AOC, Operational Employment – Air and Space Operations Center, November 1, 2007

Therefore, Combat Operations monitors real time employment of the ATO, and responds to dynamic and changing situations on the battlefield.[13] Deviations under their purview include changing targets, re-planning unsuccessful missions, reacting to emergency situations, and/or diverting aircraft for troops in contact with the enemy. During

[12] Daniel J. Hughes, *Moltke on the Art of War: Selected Writings* (New York, NY: Random House Ballantine Publishing, 1993), 92.
[13] AFTTP 3-3.AOC, *Operational Employment – Air and Space Operations Center*, 5-1.

the execution period, Combat Operations also responds to targets not originally on the ATO, referred to as time sensitive or dynamic targets.[14]

Deviating from the ATO is not a decision made lightly, and several specially designed offices aid the assessment and decision making processes. Aside from discussions about legalities, overall impact, collateral damage, and desired effects, there are several important factors to consider. First, a deliberation occurs that compares the benefits and projected outcomes of one event with another. The decision to divert an aircraft rests on risk and trade-offs. The accomplishment of one mission comes at the sacrifice of another. In some instances, the aircraft may not be able to provide coverage or close air support to ground forces. In other instances, the decision may mean not prosecuting another target or the original target.

Responding to an emerging target introduces various types of risk. First, the pilot may not be familiar with the area, and it may have unknown defenses that pose a threat to the aircraft. It is also likely no mission planning has occurred, and the aircraft and its munitions may not be the ideal solution set. Timeliness and the demand for a quick decision may further build upon the already inherent risks. Factors such as how fast an aircraft can travel, how long it will take to arrive in the area, how much fuel the pilot has onboard, and the inclusion of additional support assets also enters the decision cycle. All of the complexities of trying to control uncertain environments contribute to the assessment of cost versus benefit, and the COD pulls all the applicable pieces together to make the best possible decision when deviating from the ATO.

The liaisons in the AOC are the final members most closely tied to the ATO. An LNO's primary mission is to keep their home unit informed

---

[14] The DoD Dictionary of Military Terms describes "dynamic targeting" as attacking a target identified too late to deliberately plan for (retrieved from http://www.dtic.mil/doctrine/dod_dictionary/ on February 1, 2012.)

of operations (although they are not the formal notification medium), and to provide subject matter expertise and coordination capability to the JFACC's staff.[15] Despite not having a formal role in all of the processes, they do fulfill a vital position. Their weapon systems knowledge is especially important in the MAAP/ATO development,[16] deconflicting operations, contributing to dynamic targeting decision making, and mission execution.[17] The AOC depends on the LNOs to provide skilled knowledge and contribute solutions. Conversely, the home units depend on the LNOs to ensure the platforms are not assuming too much risk or performing unintended roles. Balancing the needs and demands of both sides illustrates the importance of the LNOs.

Command and Control Relationships

Moving away from how the warfighter tasks air assets, the stage is set for understanding issues dealing with command and control of the aircraft. Four models best delineate the different types of command relationships and control authority: In-Theater Forces, Transient Forces, Functional Forces, and Out-of-Theater Forces. The four different types of forces comprise the actors executing and supporting the ATO, and working their way across the bridge.

In-Theater Forces are the Airmen and units typically found in the AOR. An example of these forces is the personnel that comprise the AOC staff. Briefly, In-Theater Forces deploy to a location and normally transfer administrative control (ADCON), tactical control (TACON), and operational control (OPCON)[18] authority to the JFC.[19] Just the opposite

---

[15] AFDD 2, *Operations and Organization*, 72.
[16] AFTTP 3-3.AOC, *Operational Employment – Air and Space Operations Center*, 4-43.
[17] AFTTP 3-3.AOC, *Operational Employment – Air and Space Operations Center*, 5-4.
[18] The DoD Dictionary of Military Terms describes all three types of control (retrieved on 25 Jan 12 from http://www.dtic.mil/doctrine/dod_dictionary/). Summarizing the entries, ADCON refers to "direction or exercise of authority over subordinate or other organizations in respect to administration and support." OPCON refers to "the authority to perform those functions of command over subordinate forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction necessary to accomplish the mission";

is true for Transient Forces, who represent members traveling through an AOR and are not assigned to the JFC. Outside of an emergency or legal situation, the JFC does not receive OPCON, TACON, or ADCON authority for the Transient Forces.[20]

The third model, Functional Forces, applies to forces whose mission requirements cross multiple AORs and are thus best centrally controlled. Space forces are one example, and will be discussed in more detail in Chapter 2. Cyber forces are another example, and Chapter 3 will illustrate their command and control structure. From the JFC's perspective, an important aspect of Functional Forces is that they act as a "supporting command" to the JFC, the warfighter (the "supported command").[21]

Finally, the fourth model is Out-of-Theater-Forces and can be broken into two types. The first is Outside the Continental United States (OCONUS) based forces. This group reflects launching and recovering aircraft in one overseas AOR but performing their missions in another. Normally OPCON of OCONUS forces transfers forward to the JFC when the aircraft begin the mission, but ADCON remains with the original commander. At the conclusion of the mission, the returning aircraft transfers OPCON authority back to the originating unit.[22] An example would be B-52s operating out of Diego Garcia and prosecuting targets in Iraq. OPCON shifts back and forth from Pacific Air Forces (PACAF) to Air Forces Central (AFCENT), and ADCON always remains with PACAF.

The second type of Out-of-Theater-Forces is Continental United States (CONUS) based forces. Similar to the OCONUS based forces, the

---

finally TACON refers to "command authority over assigned or attached forces or commands, or military capability or forces made available for tasking, that is limited to the detailed direction and control of movements or maneuvers within the operational area necessary to accomplish missions or tasks assigned."

[19] AFDD 2, *Operations and Organization,* 57.

[20] AFDD 2, *Operations and Organization,* 58.

[21] AFDD 2, *Operations and Organization,* 58.

[22] AFDD 2, *Operations and Organization,* 58.

assets reside in one AOR but demonstrate the Air Force's global strike capability by conducting operations in another. In these situations ADCON always remains with the parent major command while OPCON "*should* transfer . . . to the supported combatant commander/JFC upon sortie generation."[23] As will be shown later, the word "should" offers flexibility to the commanders but also obfuscates command and control issues. The example of this is the B-2 strikes in Kosovo where ADCON remained with United States Joint Forces Command (USJFCOM) and OPCON transferred back and forth to United States Forces Europe (USAFE).[24] The important takeaway for the four types of forces are that regardless of whether the JFC receives OPCON, TACON, or ADCON authority, to get in the fight – to get on the bridge – the forces answer to the AOC.

Before reviewing the B-2 employment in Operation Allied Force, it is helpful to understand how the supported command calls forces forward. The JFC's process for employing forces begins with utilizing the forces assigned by the Secretary of Defense in his "Forces for Unified Commands" memorandum.[25] If the JFC requires more apportioned forces or lacks a particular capability, the COCOM staff drafts a request for forces (RFF). The Joint Chiefs of Staff evaluate the request and submit a recommendation to the Secretary of Defense, who is the only DoD authority authorized to transfer forces between combatant commanders. Before signing the deployment orders he carefully articulates the command relationships and OPCON authority.[26] Rarely are functional forces (such as space assets, tankers, and stealth aircraft) "chopped"[27] to geographic commanders.

---

[23] AFDD 2, *Operations and Organization,* 57.
[24] Lt Col Thomas Hatley, interview by author, Maxwell AFB, AL, December 12, 2011.
[25] AFDD 2, *Operations and Organization,* 56.
[26] AFDD 2, *Operations and Organization,* 44 & 56.
[27] "Chopped" is military jargon for change of operational control (CHOP). JP 1-02, *Department of Defense Dictionary of Military and Associated Terms*, November 8, 2010 (as amended February 15, 2012).

The functional combatant commander normally maintains command of the forces to maximize efficiencies and provide global capabilities. That commander is able to prioritize resources and requests, and gain efficiencies by commanding and controlling the entire force at once. Nevertheless, there are procedures for atypical situations of transferring functional forces to geographic commands, specifically to JFCs. To make the case of transferring functional forces to geographic commanders, the requirement for the forces/effects must outweigh the efficiency and effectiveness of the functional command's mission. As mentioned previously, only the Secretary of Defense can make the decision to transfer the forces, as well as to grant OPCON or TACON control of the attached forces.[28]

One nuance that deviates from this orderly process applies to time sensitive planning for global strike missions. As the owner of global strike assets, United States Strategic Command (USSTRATCOM) is responsible for planning any courses of action (COA) involving their use, regardless of the AOR they operate within. USSTRATCOM works with the JFC's Combat Plans Division in developing COAs and providing kinetic and non-kinetic support to the possible missions. Once the Secretary of Defense selects a COA, he decides the supported-supporting relationships and which commander exercises OPCON of the mission,[29] and both staffs work together to integrate all the air and space forces.[30] Despite placing high priority on planning stealth and long-range bomber missions, the length of time required for out-of-theater aircraft to arrive over the target, often forces the aircraft to launch prior to publishing and distributing the ATO. For reasons like this, the importance of the LNO

---

[28] AFDD 2, *Operations and Organization,* 59-60.
[29] AFTTP 3-3.AOC, *Operational Employment – Air and Space Operations Center*, 3-21 – 3-22.
[30] AFDD 6-0, *Command and Control,* June 1, 2007 (incorporating Change 1, July 28, 2011 and retrieved from www.e-publishing.af.mil), 14-15.

cannot be underestimated.[31] The LNO is critical in these scenarios to keep home units apprised of plans under development and also ensure the AOC staff is not inappropriately utilizing the aircraft.

Whether the JFC is in a supported or supporting role (for unique missions, such as global strike), all the forces are presented under a single Airman in the AOR. This ensures unity of command for all the Air Force's warfighters. Likewise, the AOC maintains the Air Force's tenets for centralized control and decentralized execution, to "exploit the speed, flexibility, and versatility of global air and space power."[32] With an understanding of how forces are normally apportioned and controlled under the AOC and laid against the backdrop of control and execution, the B-2's use in Kosovo in 1999 offers an example of this system in action.

Delivering Effects: Operation Allied Force

In response to repeated failed attempts to stop Slobodan Milosevic from butchering the ethnic Albanians in the Serbian Republic of Yugoslavia, the North Atlantic Treaty Organization (NATO) and the United States launched an intervention mission entitled Operation Allied Force (OAF).[33] Early on, a decision was made to exclusively conduct an air campaign. The goal hinged on two overarching war objectives. The intent was to force President Milosevic to withdraw from Kosovo, and to rescue/recover over a million refugees. Both were extremely challenging objectives, especially when only utilizing airpower. Ultimately, the campaign lasted 78 days and OAF proved to be a pivotal war for demonstrating the effectiveness of airpower.[34]

Returning to the analogy, the suspension bridge connected the political resolve of NATO and the United States to the heart wrenching

---

[31] AFTTP 3-3.AOC, *Operational Employment – Air and Space Operations Center,* 4-65.
[32] AFDD 6-0, 12.
[33] Although widely known as Operation Allied Force, the American participation is sometimes referred to Operation Noble Anvil.
[34] Benjamin S. Lambeth, *The Transformation of American Air Power* (Ithaca, NY: Cornell University Press, 2000), 181.

atrocities in Kosovo. President Cinton's decision to not employ ground forces, however, restricted planning efforts. His public declaration to not use ground forces had two effects. First, it narrowed the width of the bridge, only requiring three lanes: one for the Air Force, one for the Navy, and a third for the air forces of the NATO coalition. Additionally, it increased the requisite for strength and resiliency. With the land and sea power lanes removed from the war plans, the air campaign needed additional reinforcement to ensure it survived the additional pressures to succeed.

Yugoslavia possessed formidable defense capabilities and aircraft. Planners in the Pentagon believed the coalition could suffer as many as 10 aircraft losses in the opening strike.[35] To prepare the battlefield and dismantle the country's defenses, the first wave of attacks was restricted to Tomahawk and conventional air-launched cruise missiles. The assets were lobbed from well outside harm's way. Later, 120 attack sorties destroyed 40 Serbian targets and downed 3 MiG-29s.[36] Despite the success of the entire coalition, the hero in the fight was just making its combat debut. The B-2 Stealth Bomber was the first manned aircraft to penetrate the defenses and ultimately proved to be the most effective and consistent performer in OAF.[37]

B-2s were (and still are) considered a functional capability, and belonged to USJFCOM for tasking. Air Combat Command maintained the mission to train and equip the aircrew, support personnel, and aircraft.[38] During OAF, USJFCOM held the leash for wartime taskings and worked with the Secretary of Defense and JFC to launch missions. Either through the original deployment order or through an RFF, six B-2 bombers were apportioned for OAF missions.

---

[35] Bruce W. Nelan, "Into the Fire," *Time Magazine,* April 5, 1999 (retrieved from www.ebscohost.com on January 27, 2012).
[36] Benjamin S. Lambeth, *The Transformation of American Air Power,* 183-184.
[37] Benjamin S. Lambeth, *NATO's Air War for Kosovo: A Strategic and Operational Assessment,* Arlington, VA: RAND, 2001), 89.
[38] The train and equip role is designated to Air Force Global Strike Command today.

As functional assets with a global strike mission, the 509th Bomb Wing's B-2s were not solely assigned to the JFC. Falling under the command and control model of Outside-of-Theater Forces, the assets remained at Whiteman Air Force Base for launching, recovering, and maintenance, but conducted their missions in Kosovo. Interestingly, unlike the guidance in AFDD 2, the aircraft did not operationally belong to the JFC at sortie generation. Rather, USJFCOM maintained OPCON of the B-2s until they crossed the Prime Meridian.[39] Forty-five degrees west longitude became the point that OPCON authority transferred between the two combatant commanders.

Despite the slightly unusual OPCON practice, the B-2 quietly enjoyed huge successes that were not fully realized until after the war. The first success was delivering the Air Force vision and promise of "Global Reach," for the first time since inaugurating the slogan.[40] Conducting 30-hour sorties and flying halfway around the world (and back) without landing demonstrated the persistent operations of the platform. The missions were extremely complex, often forcing the B-2s to launch 14 hours ahead of the support packages.[41] Adding aerial refueling, weather, night-time operations, and operating off of precisely timed scripts made for the most advanced and complicated missions ever executed. Despite only flying 1% of the sorties for the war, the stealth platform destroyed 11% of the targets with 33% of all the Precision Guided Munitions (PGMs) employed in the war, and produced a 96% weapons effectiveness rating.[42]

The second success of the B-2's performance was the ability to maximize each penetration into the country. Lt Gen Michael Short, NATO's air component commander, came to expect and rely on the B-2

---

[39] Lt Col Thomas Hatley, interview by author, Maxwell AFB, AL, December 12, 2011.
[40] Benjamin S. Lambeth, *NATO's Air War for Kosovo,* 93.
[41] John A. Tirpak, "With Stealth in the Balkans," *Air Force Magazine,* October 1999, 23-24.
[42] David Atkinson, "B-2s Demonstrated Combat Efficiency Over Kosovo," *Defense Daily,* July 1, 1999.

to hit 16 different targets with each sortie. Tying the ghostly, near-invisible aircraft to the pin-point accuracy of new 2,000 lb. PGMs allowed for never-before-seen results. The precision and technology allowed for the aircraft to drop most of the GBU-31s from 40,000 feet, unaffected by the weather, dark skies, and cloud coverage.[43] By synthesizing the two technologies, the allies ensured high precision targeting with minimal collateral damage and risk. In the day and age of instantaneous news streams, both effects were quick to become commonplace expectations.

The bomber community also broke paradigms regarding enroute or flex targeting. Initially, as many as four days went into mission planning. The dedicated time focused on analyzing threats, studying imagery, and developing tactics. After the opening weeks of the campaign, delays in the target approval process and the emergence of dynamic targets forced mid-flight deviations to pre-planned B-2 strikes or even launching without targets. The new tactics of "flexibility" countered the deeply engrained culture of nuclear-focused checklists and deliberate planning.

Flexible targeting soon characterized the OAF campaign.[44] To lead-turn the change in mission planning, General John Jumper, the Commander of United States Air Forces Europe, personally flew to Whiteman Air Force Base to speak to the crews.[45] In addition, to provide expertise in the planning cells, Lt Gen Short integrated a B-2 pilot into his team as an LNO. The pilot provided invaluable interface between the AOC in Vicenza, the squadrons at Whiteman, and the pilots in the air.[46] The proven capability of changing targets "on the fly" led to changes in

---

[43] Benjamin S. Lambeth, *NATO's Air War for Kosovo,* 90-91.
[44] Although changing targets enroute was not new to air operations, its debut as a common operating procedure in OAF became a mainstay of air operations in subsequent campaigns.
[45] Benjamin S. Lambeth, *NATO's Air War for Kosovo,* 90.
[46] John A. Tirpak, "With Stealth in the Balkans," 25-26.

the equipment carried on board the B-2, allowing greater capability to conduct mission planning real time and enroute to the AOR.[47]

For all the successes the B-2 earned, the new dynamic targeting tactics introduced a number of areas of concern that are especially pertinent in the way the military thinks. First, while dynamic targeting enabled aircrews to launch without preplanned targets or change targets enroute, the tactics encouraged and could later reinforce the philosophy of delaying decision making and allowing the decision makers to change their minds. Or worse, it could set a precedence that mirrors the command and control challenges in allowing live Predator feeds to constantly manipulate real-time operations. Additionally, the great distances the B-2 traveled set a precedence that afforded time to shift priorities and chase new ideas, and that timetable may not always exist. An aircrew operating much closer to the battle zone does not have the same luxury of altering plans on the way to the target. The more the practice occurs, the more the decision makers become accustomed to delaying final decisions or changing their minds. In many ways, this shift in timing resembles a double-edged sword. Depending on circumstances, delayed or changed decisions could be good or bad.

A habitual byproduct of becoming accustomed to delaying or changing targeting plans is an increased risk assumed by the aircrews and forces. Shortening the window for mission planning results in fewer tactical options and increases the danger to execute the mission. In instances like this, aircrews are placed at a disadvantage by flying missions without intelligence and imagery that would be afforded along traditional mission planning timelines. The imposed sacrifice may not be intentional. It may be due to limited means of receiving the information in the aircraft, or even a lack of time for analysts to fully assess the target area. For instance, during OAF the B-2s lacked direct satellite

---

[47] John A. Tirpak, "With Stealth in the Balkans," 28.

links to help navigate surface-to-air-missile threats.[48] In an interview for *Air Force Magazine*, Colonel Donald Higgins, 509th Bomb Wing Vice Commander, commented, "We have tremendous dependence on mission planning. We have to know where the threats are; we have to compare those threats with our stealth capabilities and what our vulnerabilities are."[49] Translation: Providing greater flexibility comes at the cost of aircrews incurring greater risks.

The same B-2 characteristics that give the bomber a decisive edge also creates a false impression of invulnerability. The stealth bomber is not invisible; Colonel Higgins was quick to point out, "stealth is low observable."[50] This distinct difference cannot be dismissed during combat operations. The more success the platform enjoys, the more the tendency to push the limitations and levels of risk. Likewise, the B-2's success in high precision attacks with little or no collateral damage has become the everyday expectation. Benjamin Lambeth asserted the B-2 attacked key targets with "high confidence and little risk" throughout the campaign in Kosovo.[51] Given the limited employment of the B-2, the assumption of great confidence and minimal risk will spill-over into the next conflict and the foreseeable future. Each success further promotes the belief of invulnerability, and there should be greater concern with that conviction. As infrastructure ages and technology catches up, the competitive advantage gap will close. This concept applies to all weapon types and domains.

A fourth take away from the B-2s in OAF concerns OPCON authority. Contrary to Air Force guidance, OPCON of the B-2s did not transfer to USAFE upon aircraft generation. There are plausible scenarios where the functional command will need to maintain OPCON of its aircraft throughout a mission, but that was not the case for OAF. The

---

[48] Benjamin S. Lambeth, *NATO's Air War for Kosovo,* 93.
[49] John A. Tirpak, "With Stealth in the Balkans," 28.
[50] John A. Tirpak, "With Stealth in the Balkans," 28.
[51] Benjamin S. Lambeth, *Transformation of American Air Power,* 158-159.

B-2s were provided to USAFE, who was the supported command. As such, normally the aircraft transfer OPCON authority upon aircraft generation. For OAF, the B-2s did not transfer OPCON until they crossed 45 degrees west longitude. From a command and control perspective there are a number of scenarios with this scenario that increase the chances of confusion and chaos. Operationally, if targeting information changes before the Prime Meridian, than USJFCOM should make the decision and transmit the information (or at least transmit decisions through USJFCOM). If however, the target changes after crossing the Prime Meridian, the information should come from USAFE and its planners.

For preplanned targets, command and control of the mission probably does not require a lot of changes and updates. However, in the OAF scenario the B-2s were potentially taking off without a target, or had entire strike packages changed enroute. Compounding the effects of dynamic/delayed targeting and unusual transfer authority is the fact that there were multiple B-2s in the air at the same time, each with their own target locations. It is not hard to imagine the potential confusion in getting different guidance from different locations for different aircraft, and how the confusion becomes magnified in and around the point of OPCON transfer. This is why it is traditionally recommended that command and control is transferred to the JFC upon aircraft generation. Simply put, upon stepping in to the aircraft and commencement of the mission the asset should belong on the bridge. Command and control of the bridge belongs to the JFC.

The final area of concern, or lesson learned from OAF, is whether the AOC construct is set-up to keep pace with the war. Normally the AOC has four ATOs in work. While one is under development, a second is being finalized, a third is being executed, and a fourth is being analyzed to measure the effects. The established process obviously did not match the conduct of operations in OAF. Aircraft continually

launched without targets or had targets changed enroute. Questions need to be raised as to whether the utility of dynamic targeting outweighs calls for a reform of the deliberate planning processes of the AOC. Based on the discourse about B-2s in Kosovo, airpower has proven to be able to deliver kinetic effects, and those effects are scalable relative to: precision of munitions, number of munitions dropped on each target, and how many times a target is prosecuted. Airpower has also proven to be persistent in its ability to conduct missions, but does not have great persistence of remaining in the target area. Despite how fast the leadership is able to select a target, the supersonic air platforms require a measurable amount of travel time.

Airpower functional assets possess global reach, like the B-2, but are normally restricted to night operations and require a significant amount of time to traverse the globe. Airpower has demonstrated the ability to be flexible, and the scheduling and tasking process is adaptable enough to meet the evolving need for dynamic targeting. Another distinguishing trait is the gradual escalation in risk assumed by aircrews to meet an increase in flexible targeting, despite expectations of increased precision and low collateral damage. Finally, the B-2s have illustrated that airpower remains geographically bound. Despite incredible mission capability rates in OAF, the assets require a significant amount of time getting ready for and arriving at a target, compared to the negligible amount of time spent over the target. The effects delivered are also restricted to a finite number of kinetic targets based on the payload of the aircraft.

On the evolutionary timeline of technology and domain acceptance, space is the next frontier. How does command and control change as technology becomes more advanced and the delivery of effects becomes near instantaneous? How do those answers compare to command and control of the air and relate to cyberspace?

Chapter 2

JSpOC and the Space Domain

Failure to master space means being second best in every aspect, in the crucial arena of our Cold War world. In the eyes of the world first in space means first, period; second in space is second in everything.
-- President Lyndon B. Johnson

. . . we showed and proved during DESERT STORM, and proved again during the air campaign over the Balkans, space is an integral part of everything we do to accomplish our mission. Today, the ultimate high ground is space.
-- General Lester P. Lyles

The AOC construct was useful for understanding how airpower organizes to deliver effects. Whether planning offensive and defensive actions, the JFC owns the entire kill chain process, from targets to assets to authorization for prosecuting missions. The means of executing missions happen by way of kinetic weapons at subsonic speeds. Aircraft are the instruments of delivering effects, but the utility of the aircraft are limited. They are limited because their range and capability for causing effects is restricted to the area of the aircraft upon launching the weapons. Its utility is also closely tied to space superiority.

Space touches nearly every part of the battlefield, and is integrated into the aircraft and latest weapons. In this regard, the utility of space and the speedy delivery of effects are appealing to the JFC. Space-based assets are able to support customers all over the world and provide near real-time effects. Based on its range and scope of operations, the command and control model for space provides another model to contrast with cyberspace.

Before jumping into how space is organized, it is useful to picture all the ways satellites contribute to the fight and how they tie into the bridge. The cyber bridge is starting to take form. The deck represents

the warfighters, the length symbolizes the distance the forces travel, and the width portrays the size of the force brought to bear. One lane for each service or component. The span of control travels through the suspension cables, allowing the commander to communicate and direct the forces. The next part of the construction represents space's contribution to the structure.

Space provides all the markings, lights, signs, flags, and weather sensors installed on the bridge. The lines between the lanes provide positioning and orientation perspective. The electronic signs provide important information and answers important questions. What lies ahead? Does this lane merge or end? When is the next exit? Or is there an accident or road block? The atmospheric sensors and measurement devices provide critical weather data that the operators require to complete their missions successfully.

Possessing a perspective and vantage point that provides a global perspective from a position that supersedes geographic boundaries entails space's contribution to the fight. Often described as the ultimate high ground, space has changed the battlefield. Space introduced the capability to visually go behind the scenes and collect information, to monitor and predict changing weather conditions, to enable secure communications around the globe, to tell Airmen where they were standing, and sometimes more importantly, where the enemy was hiding. In the past, the high ground was the dominant position on the battlefield, and afforded an advantage over the enemy. Today space represents that high ground and makes indispensable contributions every day. Smart weapons, like the Joint Direct Attack Munition (more commonly referred to as JDAM), made their debut with the B-2 in Kosovo, and forever changed the way leaders plan for warfare. No country comes close to matching the United States' commitment to

developing space power, and is more effective at exploiting its advantages for the warfighter.[1]

There are a number of attributes that make space unique. First, space acts as a conduit for "terrestrial- and celestial-based movement and transfer" of information and capability.[2] John B. Sheldon and Colin S. Gray highlight how space assets are exclusively able to provide global coverage with minimal assets.[3] Further, in creating a constellation of interconnected assets, spacepower is sometimes capable of providing a continuous, unblinking view of parts of the world. The ability to operate without overflight concerns enables global coverage. Through space assets, the United States is able to maintain a global presence anywhere in the world and often for as long as it is required. With a growing reliance on indispensable space products and persistent presence, control of the space domain becomes critically important.

Debate occurred as to whether space was a domain, because it did not possess the traditional characteristics associated with air, land, and sea.[4] Discussions and personal opinions in military circles lost their relevance when Joint and Air Force doctrine hooded the space environment as the fourth domain – air, land, sea, and space. First in AFDD 2-2, and now in AFDD 3-14, space is a domain within which military conducts operations. JP 1-02 reinforces recognition of the space domain, where "military activities shall be conducted to achieve US national security objectives."[5] President George W. Bush echoed the connection between space and national security, illustrating how space

---

[1] James Clay Moltz, *The Politics of Space Warfare: Strategic Restraint and the Pursuit of National Interests* (Stanford, CA: Stanford University Press, 2008), 1.
[2] John J. Klein, *Space Warfare: Strategy, Principles and Policy* (New York, NY: Routledge, 2006), 60.
[3] John B. Sheldon and Colin S. Gray, "Theory Ascendant? Spacepower and the Challenge of Strategic Theory" in *Toward a Theory of Spacepower: Selected Essays* (Washington, D.C.: National Defense University Press, 2011), 8.
[4] Everett C. Dolman, "New Frontiers, Old Realities," *Strategic Strategies Quarterly*, Spring 2012, 85.
[5] JP 3-14, *Space Operations*, January 6, 2009 (retrieved from http://www.fas.org/irp/doddir/dod/jp3_14.pdf on February 16, 2012).

superiority needs to go beyond being a force multiplier and focus on true space control;[6] the ability to "attain and maintain a desired degree of space superiority" to "ensure freedom of action in space for the United States and its allies and, when directed, deny an adversary freedom of action."[7] All other domains have grown dependent on space superiority. Without space integration, the warriors on the cyber suspension bridge would become secluded and blind. They would only be able to project, see, and interpret as far as the naked-eyes would permit on a clear, sunny day. A dominating presence in space is essential to exploiting power advantages in the other domains.

The concept of freedom of action in space is similar to that in the air and at sea, where control does not need to be permanent and absolute. The level of control must only be enough to ensure friendly forces can accomplish their mission and achieve their objectives.[8] In this way, control needs to be temporary and localized. Sometimes merely having a presence (when no other country has one) provides unrestricted control of it; the presence alone is enough to exercise control.[9] Air Force doctrine denotes space *superiority* does not mean that the enemy cannot interfere with the operations, just that the enemy cannot impact the outcome. Even when addressing space *supremacy*, doctrine caveats that the enemy may rely on small pockets of unfettered capabilities or third-party assets to achieve localized successes elsewhere in space.[10] This outlook mirrors Corbett's perspective of the sea.[11] Given the vastness of the domain and the level of technology, permanent and absolute control

---

[6] Joan Johnson-Freese, *Space as a Strategic Asset* (New York, NY: Columbia University Press, 2007), 9.
[7] AFDD 3-14, *Space Operations*, 5 & 54.
[8] John J. Klein, *Space Warfare*, 24-25 & 66.
[9] John J. Klein, *Space Warfare*, 61.
[10] AFDD 3-14, *Space Operations*, 7 & 55-56.
[11] Julian Corbett, *Classics of Sea Power* (Annapolis, MD: Naval Institute Press, 1911) 102.

is not only unachievable but would produce a diminishing return of effort and resources.

Michael Sheehan captured Gen Lance Lord's (Commander, Air Force Space Command) thoughts on command and control of space during an Air War College address. "We will dominate our opponent in space . . . and just as our Air Force doesn't continually dominate the international skies, we haven't, and aren't going to dominate all of space." Gen Lord further likened the space domain to controlling sea lanes and air space in wartime.[12] Because the other terrestrial domains rely so heavily on space's ability to persistently support daily and wartime operations, the command and control of space power is critically important.[13]

There are two views of space power. The first presents space as a physical environment for space-centric activities. The second presents space from an effects-centric view. Whereas the first portrays forces employed at the tactical, operational, and strategic levels. The effects-based lens purely focuses on the end results at the operational level.[14] The philosophy linking the two is that the JFC can plan to achieve operational effects without directing how to employ the assets. In other words, like with aircraft, there is a means to exercise centralized planning and control with decentralized execution. Just as the AOC plans and decentralizes the execution to the wings, the Joint Space Operations Center (JSpOC) builds the plan and empowers the home units to employ the plan.

Also like the AOC, the JSpOC is postured to provide planning and coordination between the space community and the warfighter; to deliver space power to the battlefield. The remainder of this chapter will

---

[12] Michael Sheehan, *The International Politics of Space* (New York, NY: Routledge, 2007), 113.
[13] John B. Sheldon and Colin S. Gray, *Toward a Theory of Spacepower: Selected Essays,* 10.
[14] AFDD 3-14, *Space Operations,* 3-4.

examine the organizational construct of the JSpOC, how it orchestrates command and control, and the delivery of effects.

Organizational Construct: The JSpOC

Before dissecting the JSpOC, it is important to understand the utility of a military presence in space. Space assets are functional assets that fulfill single-theater, multiple-theater, as well as global objectives. Quoting Napoleon Bonaparte's famous diction "Nothing is more important in war than unity of command," a single master needs to command and control the DoD's array of space assets.

To centralize planning and control, USSTRATCOM retains overall responsibility for all military operations in space.[15] The space model is different than the AOC model, where assets are apportioned to the JFC to fight. Because space is a functional asset and able to provide support to multiple users, in multiple locations, simultaneously, control of space assets are normally not delegated to JFCs or JFACCs. In this way, space is able to not only service different users on the bridge but also users on different bridges altogether.

USSTRATCOM has seven complex and diverse mission sets and relies on sub-unified and component commanders to accomplish the mission (Figure 5). The Joint Forces Component Commander – Space (JFCC-Space) is the single point of contact for military space missions, headquartered at Vandenberg Air Force Base, California.[16] JFCC-Space integrates the military space assets from Air Force Space Command, Naval Network Warfare Command, and the US Army Space and Missile Defense Command.[17]

---

[15] Space Primer, 153 & 154-155.
[16] USSTRATCOM Fact Sheet (retrieved from http://www.stratcom.mil/functional_components/ on February 16, 2012)
[17] Space Primer, 150-151.

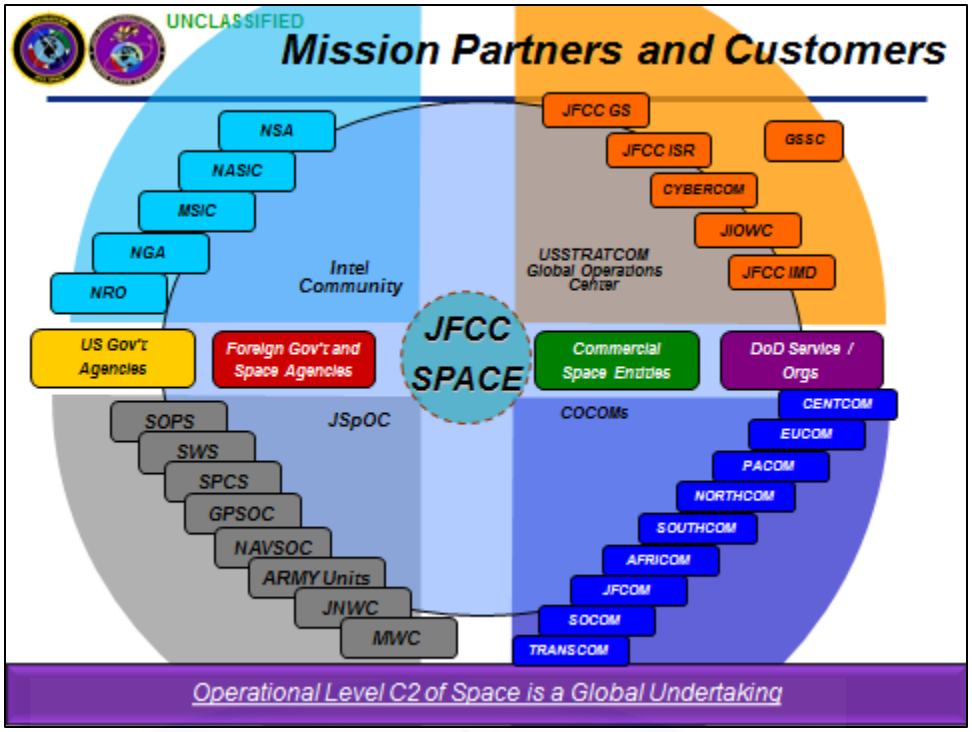

Figure 5: Mission Partners and Customers in the DoD Space Community
Source: JSpOC Overview Briefing

Space assets possess utility at both the macro and micro level of information and capability. Their ability to provide persistent presence with a global perspective differs from the terrestrial domains. Space has four primary categories: Space Control (exploiting and denying capabilities), Space Force Enhancement (products to maximize effectiveness; i.e. weather, communications, Global Positioning System (GPS), intelligence), Space Force Application (support to weapon systems; i.e. Intercontinental Ballistic Missiles), and Space Support (space launch and control infrastructure).[18]

The four categories are composed of assets that can fulfill global as well as theater support simultaneously. The forces that operate the assets, however, support either a global mission or a theater mission. Therefore, the functionality of space is traditionally broken into two categories. Space forces either provide global or theater support. An

[18] Space Primer, 82-83 & 137-142, and AFDD 3-14, 4-5.

example of global forces is GPS operators at Schriever Air Force Base, Colorado. They provide a service that requires management of an entire constellation, whose product touches all points on the globe. The GPS operators are able to support all forces by managing a global system.

On the other hand, deployed space operators in a JFC's AOC represent theater forces. Their mission is to ensure maximum integration of all space capabilities brought to bear in one particular region. To consolidate and focus all of space's potential at the regional level, a Director of Space Forces (DIRSPACEFOR) is appointed to advise the CFACC. The DIRSPACEFOR and the AOC's space support teams ensure the four space categories receive maximum integration in the war plans and execution[19] by translating the needs of the JFC and the AOC to the JSpOC, who balances requests from regional as well as global users.

The JSpOC is the JFCC-Space's "synergistic command and control weapons system focused on planning and executing." It operates as a focal point for the "operational employment of worldwide joint space forces" and integration of space effects into military missions.[20] The organization gives the commander JFCC-Space a command and control capability over assigned and attached forces, and ensures the generation of tailored space effects for military objectives.[21] USSTRATCOM receives requests from forces throughout the world, and the JSpOC is the integration point for prioritizing needs and maximizing the utilization of space assets. They accomplish the operational employment of space forces by planning, deconflicting, and synergizing products of different systems to accomplish the desired effects amongst the myriad of requests (Figure 6).

---

[19] AFDD 3-14, *Space Operations*, 7 & 16.
[20] JSpOC Fact Sheet (retrieved from www.vandenberg.af.mil/library/factsheets on January 5, 2012).
[21] JSpOC Orientation Briefing, Lt Col Scott "Stanky" Brodeur, slide 16.

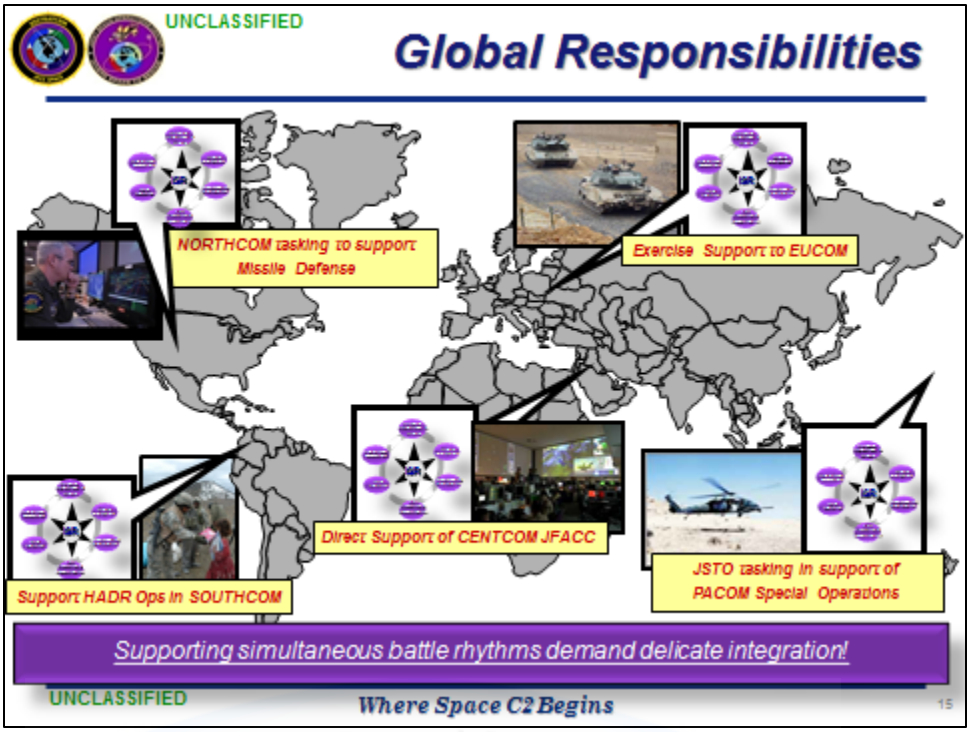

Figure 6: Space Global Capabilities
Source: JSpOC Overview Briefing

At the same time the JSpOC is turning on the lights for one bridge, it is updating hazard conditions for another bridge, ensuring heightened GPS effects on another bridge, and simultaneously ensuring weather patterns are tracked on another. In this way, as opposed to requesting a specific platform to conduct a mission, the JSpOC enables the warfighter to request an effect. The JSpOC then determines the best way to translate the requested desired effect into a desirable product.

Similar to the AOC construct, the JSpOC is comprised of four core divisions. There is a Strategy Division, Combat Plans Division, Combat Operations Division, and ISR Division. Collectively the four divisions allow the JSpOC to plan, analyze enemy space capabilities, and nominate targets.[22] Often, the dynamics of the battlefield require the JSpOC to be able to handle three types of planning: deliberate, crisis action, and adaptive campaign planning. The Strategy Division

[22] AFDD 2-1.9, *Targeting*, June 8, 2006 (retrieved from www.e-publishing.af.mil), 104.

interprets USSTRATCOM and the JFCC-Space Commander's guidance to develop long- and short-term strategies. They produce the Joint Space Operations Plan (JSOP) and the Space Operations Directive (SOD), in a fashion similar to how the AOC's Strategy Division produces the AOD.[23]

One important nuance, however, speaks to the command and control of space assets. The AOC's Strategy Division integrates any space assets that the CFACC has operational or tactical control over into the air operations plan. All other joint space assets belong to JFCC-Space and committed by the JSpOC Strategy Division, through the space operations plan.[24] With the exception of the CFACC's assets, the space operations plan prioritizes all requests for joint space support and details global and theater requirements. This includes requests from the AOC and other JFC staffs that they are not able to provide for themselves.[25] Requests are submitted for consideration, and then prioritized based on the JFCC-Space's SOD. The SOD balances the available assets and capabilities and the desired effects and weight of effort required to achieve the objectives.[26] The JSOP and the SOD are the basis for building the Joint Space Tasking Order (JSTO), produced by the Combat Plans Division.[27]

The JSpOC Combat Plans Division, like the one in the AOC, is broken into two offices that build an executable plan. The first office, called the Master Space Plan Team, uses the space plan and directive to build the equivalent of the MAAP, called the Master Space Plan (MSP). The MSP provides a visual picture of how the joint space forces are postured to support JFCC-Space, geographic and functional commanders, and JFCs. Once built, the MSP is transmitted to the second office in Combat Plans, the JSTO Production Team.

---

[23] AFDD 3-14, *Space Operations*, 30; JSpOC Fact Sheet.
[24] AFDD 3-14, *Space Operations*, 20-21
[25] Lt Col Brodeur in a personal interview, February 21, 2012.
[26] AFDD 3-14, *Space Operations*, 20-21.
[27] The JSTO was formally referred to as the Space Tasking Order, or STO.

The JSTO Production Team matches available assets and builds the executable plan, or JSTO.[28] In turn, the myriad of requests becomes a coordinated and executable plan, based on asset availability and priority. Unlike the ATO's 72-hour cycle, the JSTO production cycle runs on a 3-week battle rhythm (Figure 7). Traditionally, the Commander of JFCC-Space signs the JSTO on a Friday and disseminates it that day. The JSTO goes into effect on Sunday and – unlike the ATO, which runs for 24 hours – remains in effect for one week.[29]

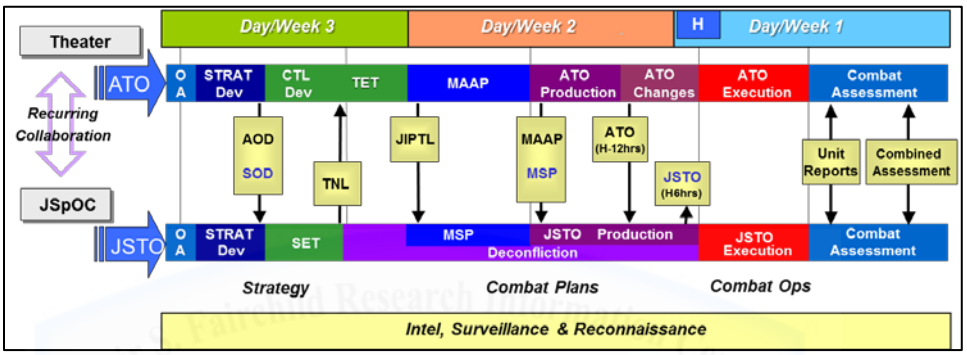

Figure 7: ATO – JSTO Comparison
Source: JSpOC Road Show Briefing for SAASS

The seamless bond between the AOC's Combat Operations Division and the space units that support the ATO through the JSTO occurs by way of the JSpOC Combat Operations Division. Once published, responsibility for monitoring the JSTO during the execution phase is turned-over to the JSpOC Combat Operations team. Monitoring the JSTO and publishing any required changes falls under the responsibility of the Combat Operations Division. In addition to maintaining real-time space situational awareness and monitoring the execution of the JSTO, the team also provides 24/7 reachback capability for the warfighters.[30] Typically a request for an unscheduled effect is relayed through the

[28] AFDD 3-14, *Space Operations*, 31; JSpOC Fact Sheet.
[29] Lt Col Brodeur in a personal interview, February 21, 2012.
[30] AFDD 3-14, *Space Operations*, 31; JSpOC Fact Sheet.

JFC's DIRSPACEFOR, directly to the Combat Operations Crew Commander.[31]

An example of an unscheduled support request occurred on July 18, 2009 when an F-15E Strike Eagle crashed in eastern Afghanistan. The JSpOC's Combat Operations team happened to be monitoring an official DoD chat site and observed messages about the downed aircraft. The team contacted several units that could offer assistance and put them on standby. Shortly afterwards, the AFCENT DIRSPACEFOR called the JSpOC to request information and potential capabilities. After receiving the official request from the DIRSPACEFOR, the Combat Operations team proceeded to directly task the standby units.[32]

A notable difference between the JSpOC and the AOC's planning and execution teams are the availability of weapon system expertise and utilization of LNOs. The JSpOC is comprised of space operators who collectively manage 54 DoD satellites.[33] Although there is a desire to have weapon system expertise integrated throughout the planning cells and employment teams, the requirement as well as the capability does not exist. Since the JSpOC does not actually operate the satellites, the desire to have expertise on the staff merely introduces an additional requirement to manage and schedule. When framed by the existing challenges of including assets and personnel from other services, adding a requirement for weapon system expertise exacerbates the problem. Also, remembering the requirement is to command and control satellites but *not* actually operate the assets, the JSpOC's direct interface with the units that *do* operate the satellites negates the need for LNOs. Essentially the only LNO is the DIRSPACEFOR.

---

[31] Lt Col Brodeur in a personal interview, February 21, 2012.
[32] Capt Allison Haas in a personal interview, February 21, 2012.
[33] Col Michael V. Smith during a class lecture, February 7, 2012.

Command and Control Relationships

USSTRATCOM maintains command and control of military space assets for two reasons. First, the global nature of the assets translates into geographically unconstrained users and utility. Integration of space assets requires a simultaneous tactical and global perspective. Second, space provides functional or desired effects capability, as opposed to a regional capability. By allowing the users to express the needed effects, USSTRATCOM decides the best way to provide the effects while also meeting the needs of all the other users. Meeting the global or multiple theater requirements often requires a command and control model that bridges theaters and merges non-military capabilities.[34] Centralized control is the most appropriate method to maximize the finite capability of the space assets. USSTRATCOM maintains COCOM of space forces and assets, and exercises the authority and operational-level effects through the Commander of JFCC-Space.[35] Collectively the two maintain command and control of the global space forces and act in a supporting commander capacity role to the supported JFC. Chapter 1 explained that there are four types of models for presenting forces to the fight; In-Theater, Transient, Functional, and Out-of-Theater Forces. Space forces are normally presented as In-Theater Forces or Functional forces.

In-theater forces include the space personnel in the JFACC's AOC. The AOC division is comprised of space operators in most offices, to offer integration and advocacy. Some of the operators reside as LNOs and provide expert advice, facilitate integration, and coordinate with home units. There are also times when forces deploy forward and transfer some ADCON control to the gaining unit, but still maintain OPCON with JFCC-Space. Normally, however, space forces remain with their home unit and perform their mission as Functional Forces.

---

[34] AFDD 3-14, *Space Operations*, 9 & 32.
[35] Space Primer, 155.

Because Functional Forces are able to meet multiple mission requirements across the globe, their capabilities are best centrally controlled. As such, the JFCC-Space Commander maintains OPCON of the assigned forces, and performs supporting command functions for the forward deployed JFC. Although space units outside the AOR may perform some missions inside the AOR, they are Functional Forces.

For larger operations, a JFC can request space effects from USSTRATCOM and the Secretary of Defense will specify a supporting/supported relationship. At times, just as with global strike assets and forces, the JFC may request OPCON for space forces.[36] The Secretary of Defense weighs the effectiveness of the regional requirements against the global effectiveness and efficiencies before deciding to transfer OPCON of space forces to the JFC. When instances like this occur, the Secretary of Defense's message will specify the type and duration of control, as well as the supported/supporting relationship.

Outside of the four models for presenting forces, the supported/ supporting relationships fall into one of four possible support categories: general, mutual, direct, and close.[37] The type of relationship is especially pertinent to the command and control of space assets, because they accentuate the priority of support without transferring actual control of the assets and units.

Generic assistance normally already provided as a whole to the supported forces characterizes the category of general support. Examples of general support include GPS and counterspace effects. Mutual support is when the supported and supporting commanders perform the same operation and rely on each other's capabilities to accomplish the mission. Direct support is when the accomplishment of

---

[36] AFDD 2, *Operations and Organization*, April 3, 2007 (retrieved from www.e-publishing.af.mil), 58.
[37] AFDD 3-14, *Space Operations*, 11.

one task requires deliberate support. For example, during OAF the AOC was directly supported by the 11th Space Warning Squadron for battle damage assessment. Finally, close support is reserved for relationships where the mission of one organization bleeds into the accomplishment of another organization.[38]

Presentation of forces and support relationships can become confusing. When the B-2 performed its mission in OAF, the supported commander gained OPCON of the asset when it delivered its effects. Space, however, normally provides effects for the supported commander without transferring OPCON. Tying it back into the bridge analogy, when the B-2 is on the bridge it cannot support other missions via other bridges. The space assets, however, are able to support multiple bridges at the same time because the assets are not physically tied to one specific operation. Therefore, the *type* of support that the JFC garners becomes important because it shifts the priority in the request for the JSpOC when it is marrying platforms and allocating time to the requests. A JFC with direct support receives higher priority than a JFC with only general support.

To maintain simplicity of coordinating space effects in the AOR, the JFC normally delegates Space Coordinating Authority (SCA) to the JFACC. Considering the JFACC has the preponderance of space forces and experience, the JFACC is a logical choice to facilitate unity of effort across the operation.[39] Additionally, the space forces are in the AOC, there is an established relationship and sequencing of plans between the AOC and JSpOC, and the CFACC is required to maintain a theater-wide perspective (over air, land, and sea).[40]

Despite the many reasons for delegating the SCA to the JFACC, that person is not a space expert. When the JFACC is the SCA, a

---

[38] AFDD 3-14, *Space Operations*, 11-12.
[39] AFDD 2, *Operations and Organization*, 62.
[40] AFDD 3-14, *Space Operations*, 15.

DIRSPACEFOR is assigned to the operations center to assist the leadership realize the full potential of the space forces. Nominated by the Commander of Air Force Space Command, the DIRSPACEFOR is critical for advising, staffing, and integrating space into the air campaign.[41] In their day-to-day capacity, the DIRSPACEFOR directly works the JFACC's space-related issues.[42]

Delivering Effects

The JSpOC is entering its seventh year of existence. The organization continues to – unsurprisingly – grow responsibility and integration into all facets of the DoD. The increasing reliance on the capabilities and successes of the space community continues to sharpen the strength of the warfighter and maintain the capabilities gap between the United States and all other nation states. Through the JSpOC, the joint space community is able to provide a persistent and global operational picture, and deliver near real-time space-based effects to the warfighter.

Pre-dating the JSpOC, the Space Operations Center provided command and control of Air Force space assets. During OAF a wide range of space capabilities enabled the many successes garnered in the air campaign. Dubbed a "War of Weather" by Admiral James Ellis (Commander, Joint Task Force Noble Anvil), GPS proved to be the unsung hero of the war. Former Chief of Staff of the Air Force, General Richard Myers was quoted as saying, "It is tough to put a price tag on the count of lives that I believe we saved due to space support in Kosovo . . . There is little question that space was vital to the allied victory."[43] Due to the bad weather, GPS-guided munitions (especially from the B-2)

---

[41] AFDD 3-14, *Space Operations*, 16.
[42] Space Primer, 161.
[43] Peter Grier, "The Investment in Space," *Air Force Magazine*, February 2000 (retrieved from http://www.airforce-magazine.com/MagazineArchive/Pages/2000/February%202000/0200investment.aspx on March 7, 2012).

were critical to conducting safe and reliable operations, and "eliminating enemy sanctuaries and operational lulls."[44]

Space planning and coordination presents an interesting paradox. Satellites are omnipresent and capable of providing products and situational awareness with little preparation or planning. Timing becomes the driving factor, as opposed to asset availability. The ability of satellite constellations to constantly remain overhead enables them to respond quickly to emerging needs and rapidly changing circumstances. The logical assumption would be that an asset with so much versatility would translate into a tight battle rhythm and short JSTO cycle. The opposite is true. The space community holds to a deliberate planning process that stretches planning into weeks.

Relatedly, the joint space community is a support element for the warfighter. In compliance with international accords, space assets are not used to offensively weaponize space.[45] The assets do provide capabilities and information that the terrestrial forces use in an offensive capacity. Again, the question arises about the battle rhythm and operations tempo. Three factors enable the space community to remain wedded to a long-range planning cycle.

First, the combination of predictable orbits and the ability to indefinitely stay aloft answers some of the concerns about supporting the warfighter. The space community is able offer a list of predictable capabilities that enables the AOC planner to predictably plan their own operations. Coupled to this, JFCC-Space's guidance is provided well in advance and enables the supported JFCs to weigh-in with arguments while the JSTO is still early in production. Since, information for prepping the battlefield and orienting the warfighters relies on products

---

[44] AFDD 3-14, *Space Operations*, 33.
[45] United Nations Treaties and Principles on Outer Space, (New York, NY: UN, 2002), 4 (retrieved from http://www.unoosa.org/pdf/publications/STSPACE11E.pdf (accessed April 10, 2012).

from space assets; the planners are able to look into the future to see what information will be available. Additionally, the planners can time sequences of events on the battlefield based on overhead capabilities from the space community. In this way, space begins to resemble the markings on the suspension bridge. Speed limit and right of way signs present situational awareness for the battlefield. Weather indicators predict conditions and provide notice to the warfighters. All available assets remain ready and waiting for the operations to commence.

Second, the myriad and number of satellites leverages a redundancy in capability. This speaks to why space forces are functional forces, and how they are able to turn effects-based requests into different products for different users all over the globe . . . simultaneously. Leveraging the flexibility, persistence, and resiliency of the constellations allows the JSpOC to provide a 24-hour reachback service for the warfighters. The reachback for support builds on the predictable planning efforts and affords a capability to help adjudicate emerging conditions and threats. In the same way, interactive signs on the bridge relay changing conditions and time-sensitive information.

The final reason the JSpOC's planning cycle works ties-in the application of direct support and direct liaison authority (DIRLAUTH).[46] DIRLAUTH fulfills the need for warfighters to convey specific instructions and request specific ways of shaping support. In the rare circumstances of granting DIRLAUTH, it is important for the JSpOC to remain engaged in the coordination and requests, so they can deconflict and plan accordingly. Additionally, the type of support directed by the Secretary of Defense – specifically direct support – ensures a stratified approach to allocating priorities to the warfighters with the greatest needs.

---

[46] DIRLAUTH is when a subordinate unit is granted authority to consult or coordinate actions directly with another agency. In the space community this happened more often before the JSpOC was established. JP 0-2, *Unified Action Armed Forces*, July 10, 2001 (retrieved from http://www.bits.de/NRANEU/others/jp-doctrine/jp0_2.pdf on February 4, 2012) and personal interview with Lt Col Brodeur.

Despite all the ways the JSpOC presents resources to the JFC, the space community still lacks recognition for its contributions. This possibly stems from two rationales. First, the JFC represents the United States' military application of force and traditionally measures success in the ability to win kinetic victories. Since space does not deliver kinetic violence, it is underappreciated for its contributions; often only thought of in the absence of everyday support. Although space enables precision strikes with less collateral damage and fewer munitions expended, the warfighter still measures the success in terms of physical destruction.

The second reason space assets struggle for recognition is due to the self-imposed cloak of secrecy. Despite instituting a DIRSPACEFOR, JFCC-Space, and peppering the AOC staff with space professionals, the warfighters are reluctant to trust what they cannot see for themselves. In Operations Iraqi and Enduring Freedom, the AOC regularly expended airborne assets to provide the same (or lesser) products than the space community already had available. Due to classifications and compartmentalized programs, the AOC planning staff rejected reliable and sometimes superior information because they could not be told from where the information originated. Due to the inability to speak plainly and reveal sources, the staff rejected the information and scheduled sorties to capture their own intelligence.[47]

Similarly, the lack of faith in space's contributions can lead to dismissing space capabilities, and selecting kinetic destruction. During OAF, space effect options were presented that would have disrupted Serbian communication systems, but the JFC wanted the physical destruction. In lieu of implementing non-kinetic effects, the conventional munitions repeatedly struck targets and resulted in the death of 53

[47] Maj Francois Roy in a personal interview, January 10, 2012. Maj Roy was the CAOC NRO Liaison and later the ISR Element Chief during OIF/OEF.

Serbians.[48] The reason this is important speaks to risk acceptance. If the warfighter does not learn to trust the capabilities, personnel executing conventional missions will continue to replace non-kinetic options with kinetic ones. Not only does this minimize the exploitation capabilities of entire weapon system, but additional risk to life is also incurred on both sides. Only through building trust in the capabilities of the space community will the warfighter truly capitalize on their ability to provide near real-time effects.

[48] Col Michael V. Smith during a class lecture, February 10, 2012. Col Smith was on the OAF AOC MAAP Team and in charge of targeting enemy communication systems.

Chapter 3

USCYBERCOM and the Cyberspace Domain

Cyberspace may be key to how the United States – and by extension, those it fights alongside – go to war . . . Taken to its logical conclusion, warfare becomes a matter of finding targets while not becoming one . . . cyberspace is the potential fulcrum for power relationships.
-- Martin Libicki

Following the progression of technology, speed, and command and control structures, this thesis moved from airpower's ability to deliver effects at sub-sonic speeds through the AOC model, to the delivery of space effects at near real-time speeds through the JSpOC. Before comparing and contrasting the air, space, and cyberspace capabilities and control structures, it is necessary to break cyberspace down and study its function, framework, command and control, and how effects from the cyber domain are delivered at the speed of fiber optic light.

The elegance of the bridge analogy really takes root with the inclusion of the cyber domain. Cyberspace is the ultimate enabler that not only exists within each weapon system, but more importantly ties them all together. The bridge's deck represents the posture of forces, transporting the military might from the United States to an AOR. The suspension cables depict the span of control exercised by the JFC. As also discussed, the signage, placarding, and weather instruments illustrate the space assets wired into the warfighter. The information provided by the spaceborne assets orient and prepares the warfighter before, during, and after mission execution.

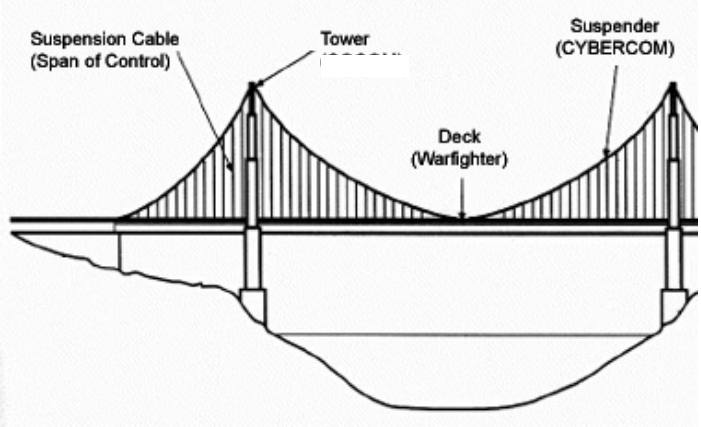

Figure 8: Suspension Bridge Diagram
Source: Adapted from
http://mmem.spschools.org/grade3science/3.bldg/Suspension.html

Cyberspace fuses the elements together and enables the JFC to mobilize and execute theater operations (Figure 8). The main suspender cable that travels the length of the bridge represents the presence of cyberspace. Cyber power empowers the JFC by providing real-time command and control communications, which ties directly into the span of control. The suspender cable that is cyberspace also ties the information from the space assets into the interactive signs, and relays the weather data to the entire AOR.

Just like space capabilities, cyber operations are becoming more and more infused in to the daily operations of all the services. The United States military and civilian sectors are increasingly dependent on the safe and secure access to cyberspace.[1] Superiority in cyberspace is synonymous with the ability to command and control, collect and disseminate information, as well as restrict access to the same information.

As in the space domain, cyberspace has come under fire as to whether it exists as a standalone domain. More so than the acceptance of space as a domain, cyberspace does and does not exist as a part of nature. In some aspects, it exists within the electromagnetic spectrum.

---

[1] AFDD 3-12, *Cyberspace Operations*, July 14, 2010 incorporating Change 1, November 30, 2011 (retrieved from www.e-publishing.af.mil), ii.

Others, however, view cyberspace as a manmade domain or phenomenon. In this regard, it requires more attention to shape and manipulate. Regardless, both diametrically opposed positions are true, and again like space . . . it does not matter. As interesting as it is to debate, command authority has anointed cyberspace as a domain. It is a "global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the internet, telecommunications networks, computer systems, and embedded processors and controllers."[2]

The DoD definition of cyberspace is embedded in doctrine, affirming the existence of the domain status and recognizing the importance of freedom of action within the domain. As a domain, cyber's utility resides in its ability to employ cyber capabilities in the achievement of military objectives, and to deliver effects through the electromagnetic spectrum. "Cyberspace nodes physically reside in all domains. Activities in cyberspace can enable freedom of action for activities in the other domains, and activities in the other domains can create effects in and through cyberspace."[3]

AFDD 3-12 edifies the imperative of winning superiority in cyberspace, highlighting that superiority represents the ability to operate without the enemy interfering with friendly operations.[4] The capacity to operate without interference is not to be confused with operating uncontested. Rather, superiority denotes the capabilities and techniques to counter attempts at interference.

Interestingly, AFDD 3-12 blends the concepts of superiority and supremacy.[5] Earlier theorists, like Julian S. Corbett and naval theorist Alfred Thayer Mahan, clearly separate the two. They denote how

---

[2] JP 1-02, *Department of Defense Dictionary of Military and Associated Terms*, November 8, 2010 (As Amended Through October 15, 2011).
[3] AFDD 3-12, *Cyberspace Operations*, 2.
[4] AFDD 3-12, *Cyberspace Operations*, 2.
[5] AFDD 3-12, *Cyberspace Operations*, 2.

superiority normally regards control as localized and temporary, as well as the ability to operate without impeding operations.[6] Supremacy, on the other hand, typically refers to broad, enduring, and absolute control.[7] Despite being man-made, the fight for uncontested supremacy in the cyber domain has the same challenges as the four other domains. The primary difference being the barrier of entry is negligible in contrast to the air, land, sea, and especially space, environments.[8]

R.A. Ratcliff presents a different perspective on control of cyberspace when she talks about security. ". . . no security can be guaranteed. We can only assume reasonable security – a system which protects information for a limited time."[9] The secret, she says, is staying one step ahead of the adversary and developing systems that can be compromised without causing a complete collapse of the network.[10] In 2010, President Obama "identified cybersecurity as one of the most serious economic and national security challenges we face as a nation, but one that we as a government or as a country are not adequately prepared to counter."[11] The President is not the only one to realize the tie between cybersecurity and national security. Perhaps more than any other country's military, the DoD is wedded to the network systems and capabilities of the cyber domain; leveraged in air, land, sea, and space.[12] If the President and Ratcliff are both correct, and considering the DoD's growing dependence on – and vulnerability through – cyberspace, the

---

[6] Julian S. Corbett, *Some Principles of Maritime Strategy* (Annapolis, MD: Naval Institute Press, 1988), 103.
[7] Alfred Thayer Mahan, *Classics of Sea Power: Selections from the Writings of Rear Admiral Alfred Thayer Mahan* (Annapolis, MD: Naval Institute Press, 1991), 190 & 295.
[8] James A. Lewis, *Thresholds for Cyberwar*. Center for Strategic International Studies. Washington, D.C., September 2010.
[9] R.A. Ratcliff, *Delusions of Intelligence: Enigma, Ultra, and the End of Secure Ciphers* (New York, NY: Cambridge University, 2006), 235.
[10] R.A. Ratcliff, *Delusions of Intelligence*, 235.
[11] Comprehensive National Cybersecurity Initiative, 2010 (retrieved from http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative on 20 February 2012).
[12] P.W. Singer, *Wired for War: The Robotics Revolution and Conflict in the 21st Century* (New York, NY: Penguin Books, 2009), 200 (Referenced in Joseph S. Nye, Jr's book *The Future of Power*), 36.

nation must fight every day for superiority.[13] Because the loss of superiority can have cascading effects into the other domains – as depicted by the main suspender cable in the bridge analogy – it is imperative for the DoD to organize itself in a way that best guarantees the chance to maintain dominance. That task begins with understanding command and control, and developing a model that balances capability with risk.

Organizational Framework: USCYBERCOM

On June 23, 2009 the Secretary of Defense issued a memorandum to the DoD. In it he directed USSTRATCOM to "establish a subordinate unified command designated as United States Cyber Command (USCYBERCOM)" to secure freedom of action in and through the cyber domain.[14] The memorandum also called for the Joint Chiefs of Staff to develop a plan to dedicate forces to the mission. The Under Secretary of Defense for Policy was designated the lead for developing a comprehensive strategy for DoD operations in cyberspace. The directive was clear in its direction for USCYBERCOM, through USSTRATCOM, to secure the DoD global information grid (GIG) and to integrate the services.[15]

Similar to the space community, the cyberspace community is capable of providing cyber effects without being on the front lines of the geographic region; even more so than satellites, cyber is not geographically constrained. Within cyberspace resides a capability of delivering effects at the speed of light; distance is not an obstacle. With the USCYBERCOM headquarters at Fort Meade, Maryland, and operational units throughout the United States, effects are delivered to COCOMs around the world through the main suspender cables (and by

---

[13] Joseph S. Nye, Jr, *The Future of Power* (New York, NY: Perseus Books Group, 2011), 118.
[14] SecDef Memo, *Establishment of a Subordinate Unified US Cyber Command Under US Strategic Command for Military Cyberspace Operations*, June 23, 2009.
[15] SecDef Memo, *Establishment of a Subordinate Unified US Cyber Command.*

extension through the spans-of-control cables on the bridge) to the warfighters at or above any location on the globe.

Approaching two years since reaching its Initial Operational Capability on May 21, 2010, USCYBERCOM is "responsible for planning, coordinating, integrating, synchronizing, and directing activities to operate and defend the [DoD] information networks and when directed, conduct full-spectrum military cyberspace operations . . ."[16] While responsible for ensuring freedom of action for the United States, USCYBERCOM is equally charged with denying the same capabilities to its enemies.

The Commander of USCYBERCOM reports directly to the Commander of USSTRATCOM, and is dual hatted as the Director of the National Security Agency (NSA). The commander's role merges the military's United States Title 10 authority with the nation's premier cryptologic intelligence agency and its' Title 50 guidelines (Figure 9).[17]

[16] US Cyber Command Fact Sheet, December 2011 (retrieved from www.stratcom.mil/factsheets/Cyber_Command/ on February 19, 2012).
[17] According to the US Code, Title 10 outlines the roles of manning, training, and employing the uniformed military, and Title 50 outlines the roles and responsibilities of the intelligence community (http://uscode.house.gov/ and P.W. Singer in "Double-hatted Around the Law: The Problem with Morphing Warrior, Spy and Civilian Roles," *Armed Forces Journal*, retrieved from http://www.armedforcesjournal.com/2010/06/4605658/ on May 12, 2012).

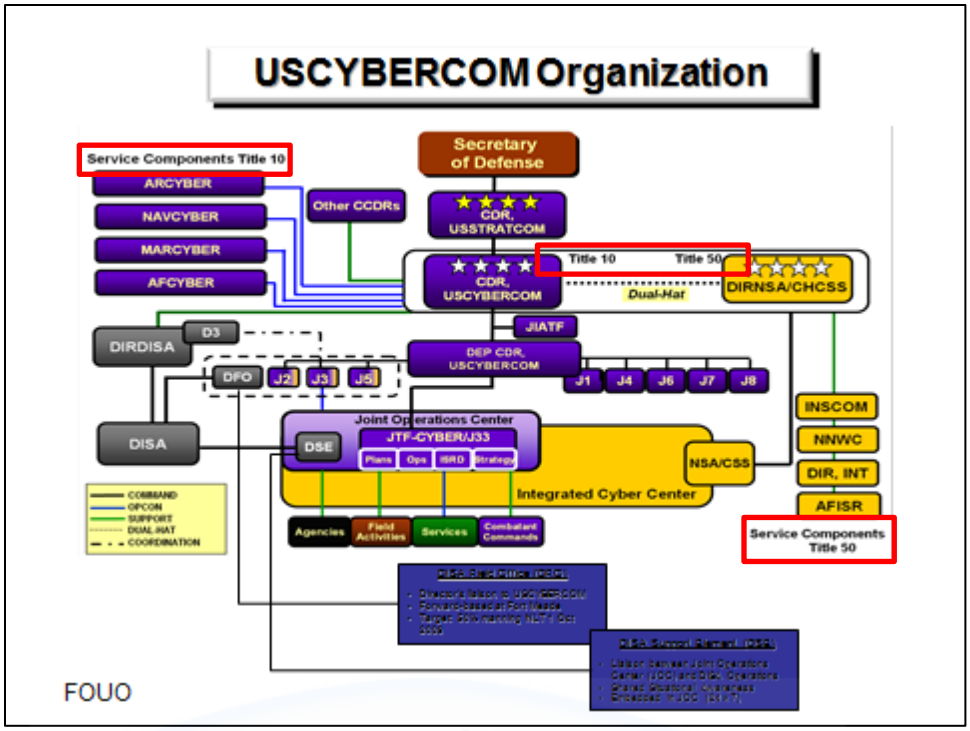

Figure 9: USCYBERCOM Organizational Diagram (FOUO)
Source: Crucial Point LLC, http://crucialpointllc.com/services/federal-services/government-markets/cybercom-org-chart/

The synergy from combining the efforts of the world's greatest military power and the country's brightest analysts offer boundless capabilities and potential breakthroughs.

The GIG is comprised of 7 million devices spread across 15,000 networks that are attacked "hundreds of thousands of times every day."[18] With its current architecture, USCYBERCOM is not able to produce a single common operating picture that enables real time monitoring and discrimination of activities on the GIG.[19] This fact was highlighted when General Keith Alexander, commander of USCYBERCOM, announced, "You can't see 'em all. You cannot defend

[18] New York Times, *Attacks on Military Computers Cited*, April 15, 2010 (retrieved from http://www.nytimes.com/2010/04/16/world/americas/16military.html on March 20, 2012) and referenced in Joseph S. Nye, Jr's book *The Future of Power*, 132.
[19] Col Robert Morris in a personal interview on February 24, 2012.

them all."[20] To manage the workload and attempt to maintain superiority of the cyber domain, each of the services handles a portion of the load by overseeing their portions of the GIG.[21]

The Armed Services provide trained personnel to USCYBERCOM through Air Force Cyber (AFCYBER), Navy Fleet Cyber, Marine Corps Cyber, and Army Cyber. Additionally, the same service commands manage their respective networks on a daily basis. Although the organizational architecture and wiring diagram for control is different for each of the services, they are expected to enforce compliance with operating instructions, monitor the effectiveness of firewalls and virus scanners, implement patches and updates to software, and educate the users on operating within cyberspace.[22]

There are three types of cyberspace operations, characterized as offensive (CNA – computer network attack), defensive (CND – computer network defense), or exploitative (CNE – computer network exploitation). Two of them follow the traditional military concepts of offense and defense. The exploitation section is more closely tied to intelligence gathering and becomes entangled in non-Title 10 responsibilities and permissions.

The request for cyber effects is modeled off the AOC and JSpOC weapon systems. Support is available through two branches: deliberate planning and reactive response.[23] An ATO-like process is the model applied to deliberately plan and employ operations.[24] The cyberspace version is the Information Tasking Order (ITO) process. Similar to the ATO process, the ITO development produces an executable 24-hour plan. The development and analysis of operations is continuous, and there are

---

[20] Noah Shachtman, *Wired Magazine*, "Military Networks 'Not Defensible,' Says General Who Defends Them," January 12, 2012.
[21] Capt Clara Bayne in a personal interview on March 19, 2012.
[22] Capt Clara Bayne in a personal interview on February 23, 2012.
[23] Capt Clara Bayne in a personal interview on February 23, 2012.
[24] AFDD 3-12, *Cyberspace Operations*, 30.

always four ITOs under construction, review, execution, or evaluation.[25] Referring to Figure 10, the purple box in the center of the diagram contains the JOC. The ITO development occurs within the J33. The J33 contains the divisions necessary for deliberately coordinating, planning, and directing cyberspace operations, as well as monitoring and responding to activities.

Mirroring the ATO and JSpOC models, the J33's Strategy Division handles long term planning while cells in the Combat Plans Division create a Master Cyber Attack Plan (MCAP) and the actual ITO. The MCAP, like the MAAP and MSP, drives the priorities and apportionment of events on the ITO.

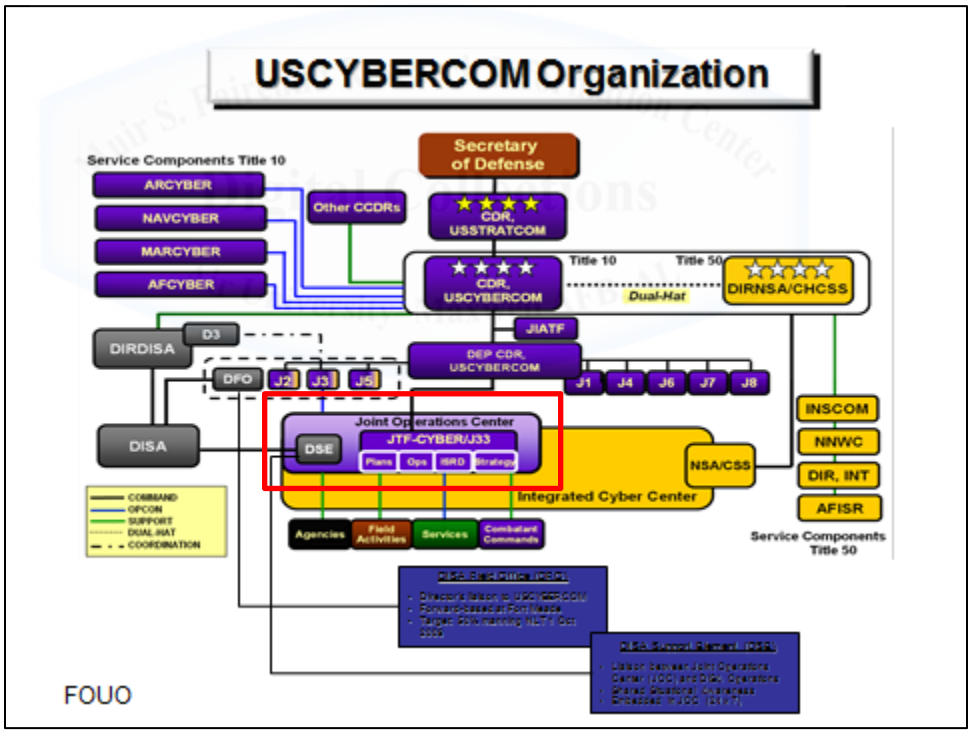

Figure 10: USCYBERCOM Organizational Diagram (FOUO)
Source: Crucial Point LLC, http://crucialpointllc.com/services/federal-services/government-markets/cybercom-org-chart/

[25] Capt Clara Bayne in a personal interview on February 23, 2012 and Maj Adam Bixler in a personal interview on March 29, 2012.

Unlike the air power process, where kinetic targets are selected from the joint integrated planning task list, cyber targets are nominated by the warfighters and submitted to COCOM Cyber Support Elements (CSE).[26] The CSEs evaluate the requests and submit Cyber Effect Request Forms (CyERF) to USCYBERCOM for planning consideration in the ITO cycle. CyERFs accepted by USCYBERCOM become missions assigned to cyber forces for execution through the ITO.[27] The ITO tasks the services' units, and they conduct the operations in much the same way an ATO tasks B-2s at Whiteman Air Force Base. Once the ITO is published, the product is distributed to the units executing the missions and to the Combat Operations Division. The Combat Operations Division manages ITO execution and responds to emerging information.

An important meeting attended by the Strategy, Combat Plans, Combat Operations Divisions, and the service components, is the daily Fires Meeting. The Fires Meeting ties the myriad of ITOs together, and highlights upcoming events and large scale exercises or operations, and tracks the effectiveness of previous missions.[28] The meeting allows for all the players to take a step back from the relentless battle rhythm – where attacks and effects are orchestrated at the speed of light – and remain situationally aware of the surrounding environment.

It goes without saying the main suspender cable allows communications to travel in both directions simultaneously. USCYBERCOM also maintains a process for handling emerging targets of opportunity or responding to unforeseen events that operates in the same way the AOC provides real-time support for the warfighter. Just like with the deliberate planning process, as needs or windows of opportunity are recognized, requests for action are forwarded to the COCOM CSEs. USCYBERCOM maintains a real-time reachback

---

[26] CENTCOM has a fully functional CSE and PACOM has a partial CSE.
[27] Maj Adam Bixler in a personal interview on March 29, 2012.
[28] Author attended Fires Meetings at USCYBERCOM February 23-24, 2012 with Capt Clara Bayne.

capability to adjudicate requests for effects and coordination with units for action.[29] In this way the process is different from the AOC which can divert aircraft or direct sorties to prosecute a target. The USCYBERCOM model more closely resembles the JSpOC in that it evaluates the needed effects and pushes the information to the "trigger-pullers."

Some of the units postured to handle real-time threats include units in the 24th Air Force, the NSA, and the Defense Information Systems Agency (more commonly known as DISA). As an example, if the AOC needed to respond to an event, the AOC would contact the CENTCOM CSE who relays the request for action to USCYBERCOM. Since the AOC is Air Force operated and has resident cyber experts deployed from 24th Air Force,[30] USCYBERCOM would likely pass disposition instructions to 24th Air Force and allow the on-site team to perform certain actions.[31] Referring back to the suspension bridge, as information travels back and forth across the main suspender cable, the correct secondary suspension cable allows corrective action to pass through the spans of control and remedy the problem.

Command and Control

Interestingly, there is not an executive agency designated for the military services in cyberspace.[32] In the absence of a lead service, each of the services is on an equal footing and reliant on USCYBERCOM for direction. Although the command is a subordinate unified command to USSTRATCOM, it exercises with similar functions and responsibilities as a fully unified command. USSTRATCOM delegates OPCON and TACON authority over cyber forces assigned to the mission.[33] In addition to exercising OPCON over assigned forces, USCYBERCOM also coordinates

---

[29] Maj Adam Bixler in a personal interview on March 29, 2012.
[30] AFDD 3-12, *Cyberspace Operations*, 26.
[31] Maj Adam Bixler in a personal interview on March 29, 2012.
[32] Lt Col David M. Hollis, "USCYBERCOM: The Need for a Combatant Command versus a Subunified Command," *JFQ*, Issue 58, 3rd Quarter 2010.
[33] AFDD 3-12, *Cyberspace Operations*, 20.

and tasks through sister services.[34] The primary missions of the command are the health and security of the critical systems, planning through the USCYBERCOM J-Staff, delivering and analyzing effects, and providing reachback assistance.[35]

USCYBERCOM provides support to operations amongst all the services and around the world.[36] When geographically located COCOMs want forces temporarily assigned to them or request specific support, "formal command relationships need to be established prior to initiation of operations."[37] Comparable to requests for aircraft or space assets, information is passed from the COCOM to the Secretary of Defense for his decision. The Secretary of Defense can decide to temporarily reassign forces to the COCOM or to designate higher levels of support for the mission. Both enable the warfighter to receive tailored support for operations.[38]

Due to the enormity and nebulous structure of cyberspace, USCYBERCOM is already dependent on the tenants of Centralized Control and Decentralized Execution. USCYBERCOM can centralize control by leading the planning, withholding permission to conduct operations, and developing initiatives to integrate and defend the networks, but must decentralize most of the execution of the operations to the service components. Maintenance, repair, and upgrades of the GIG fall on the services to manage.[39] In regards to day-to-day management, the level of involvement from USCYBERCOM is reflected in the form of information assurance vulnerability alerts (IAVAs). IAVAs are used to disseminate information about risks or vulnerabilities in the networks. They are issued by a division in USCYBERCOM that searches for vulnerabilities in the GIG and disseminates the information and

---

[34] JP 1-0, *Joint Personnel Support*, October 24, 2011, II-2 – II-3.
[35] Capt Clara Bayne in a personal interview on March 14, 2012.
[36] AFDD 3-12, *Cyberspace Operations*, 27.
[37] AFDD 3-12, *Cyberspace Operations*, 21.
[38] AFDD 3-12, *Cyberspace Operations*, 21 & 26.
[39] Maj Adam Bixler in a personal interview on February 24, 2012.

required actions. However, the command is dependent on the services to schedule and repair the vulnerabilities; most often without compliance monitoring or reporting.[40]

An example of how decentralized execution occurs can be seen by looking at AFCYBER. As the Air Force Title 10 Service Component to USCYBERCOM, AFCYBER is triple-hatted command; also carrying the titles of 24th Air Force and Air Force Network Operations. Regardless of designation, the force is comprised of over 17,500 Active Duty, Guard, Reserve, Civilian, and Contractor personnel, and broken down into five primary organizations: 67th Network Warfare Wing, 688th Information Operations Wing, 689th Combat Communications Wing, the 624th Operations Center (624 OC), and the 24th Air Force Air Component Coordination Element (ACCE).[41]

Keeping the suspension bridge's main suspender cable in mind, only certain users are permitted to take actions, and even then their actions are regulated by USCYBERCOM. For the USAF, those users are the 67th, 688th, and 689th wings. They represent the USAF's cyber forces, in which they "establish, operate, maintain and defend Air Force networks and conduct full-spectrum operations in cyberspace."[42] The 624 OC is another authorized user and acts as the command and control element for Air Force Cyberspace forces. It provides situational awareness and plan development.[43] From the operations center the 24th Air Force commander is able to exercise OPCON of the attached and assigned forces.[44] The 24th Air Force ACCE provides an important "boots on ground" coordination, advocacy, and communication presence

---

[40] Capt Clara Bayne in a personal interview on March 14, 2012.
[41] 24th Air Force Fact Sheet, April 1, 2010 (retrieved from http://www.24af.af.mil/library/factsheets/factsheet.asp?id=15663 on January 29, 2012).
[42] 24th Air Force Fact Sheet.
[43] *24th Air Force Mission Brief*, October 31, 2011.
[44] AFDD 3-12, *Cyberspace Operations*, 24.

at Fort Meade.[45] The office plays a critical role as the USAF is the only service not located at the USCYBERCOM headquarters.

In addition to proactively managing the networks, AFCYBER (as well as the other services) provide most of their own defense activities.[46] For the Air Force, to standardize networks, procedures, and responses, a significant portion of responsibilities previously handled at the base level has been centralized in the 624 OC. Complementing the 624 OC's 24-hour operations floor, the command and control element is diversified across two regional centers and one quick-response team.[47] The two regional centers are referred to as integrated network operations and security centers (INOSCs). INOSC East is located at Langley Air Force Base, Virginia, and oversees Air Combat Command, Air Force Reserve Command, Air Force Special Operations Command, Air Force Materiel Command, and Air Forces in Europe. INOSC West is headquartered at Peterson Air Force Base, Colorado, and retains responsibility for Pacific Air Forces, Air Education and Training Command, Air Mobility Command, and the Air National Guard.[48]

Each of the INOSCs provides day-to-day monitoring of the Air Force's networks and 24-hour reachback capability. Additionally, the INOSCs provide quick-reaction support to the bases and warfighters through a Computer Emergency Response Team (CERT) at Randolph Air Force Base, Texas.[49] For instance, if an Air Force base in the Pacific were to come under a virus attack, the base communications squadron would up-channel the information to INOSC West at Peterson Air Force Base. The INOSC would evaluate the threat, and simultaneously alert the CERT forces and notify the 624 OC.[50] The CERT forces on duty

---

[45] Col Robert Morris in a personal interview on February 24, 2012.
[46] Maj Adam Bixler in a personal interview on March 29, 2012 and Capt Clara Bayne in a personal interview on March 21, 2012.
[47] Capt Clara Bayne in a personal interview on March 21, 2012.
[48] Air Force News, *Air Force Stands Up First Network Warfare Wing*, July 5, 2006.
[49] *24th Air Force Mission Brief*, October 31, 2011.
[50] Maj Adam Bixler in a personal interview on March 29, 2012.

would isolate the threat, quarantine the systems, and begin forensic investigations as to where the threat originated.

As information becomes available, the 624 OC passes updates to the USCYBERCOM Joint Operations Center (JOC). In this regard USCYBERCOM is "push" rather than "pull" dependent. In order to maintain situational awareness of the GIG, the functional command relies on the services to provide information. Therefore, it is only as aware as the services enable (or allow) them to be. Perhaps this speaks to General Alexander's comments about not being able to defend the network. Without the ability to independently see the entire landscape and all the systems on the network, USCYBERCOM is hindered in its ability to protect the GIG.

Delivery of Effects

"Speed of light" is the best characterization for the swiftness in which cyberspace is able to deliver effects to the warfighter. For decades the USAF has boasted the ability to provide "Global Reach" in the delivery of airpower. Excellence in the cyberspace domain is another way that the USAF and other services can conquer distance with instantaneous cyber effects. Not only does cyber enable real-time delivery of effects, it enhances and enables the delivery of effects through the other four domains. As witnessed in Bosnia, cyber capabilities enabled B-2 aircraft to adopt enroute targeting changes. Likewise, as portrayed by the JSpOC, crews were able to leverage cyber capabilities to detect, gather, and deliver information from space assets to assess conditions with the downed F-15E aircraft. Cyberspace permits a never before seen capability to enhance or exclusively deliver effects to the warfighter.

As previously explained, USCYBERCOM decentralized most defense actions to the Air Force, Navy, Marine Corps, and Army cyber organizations, and empowered the services to defend their own portions of the GIG. USCYBERCOM, however, retains approval authority and

oversight of attack and exploitation operations. Although USCYBERCOM does not execute administrative, operational, or tactical control authority over the service forces executing attack actions, the command does retain the approval authority process for operations.[51] The sub-unified command also maintains in-residence capability to conduct attack operations.

Currently the President of the United States is the approval authority for *all* cyberattack, or CNA operations.[52] Due to the sensitivity of the connotation involved in "attacking" the enemy, General Alexander believes the authority should require presidential authority and not be granted to military commanders.[53] What constitutes an attack against an adversary's networks is still a delicate topic and largely contentious.[54] Certainly a B-2 strike against another country would require the approval of the President, and the attacked country would be expected to respond in a way commensurate with the traditional rules of war. As seen in the North Korea attack on the United States, however, the semantics and actions of warfare through cyberspace are still largely not codified. Debate is still occurring as to whether cyberspace's network boundaries deserve the same concept of national sovereignty.

What makes the cyber domain unique is that maintaining superiority is much more likely to be challenged and contested. Unlike the four other domains, the barrier of entry in the virtual world is minimal.[55] Overcoming that barrier of entry invites cyber users from around the globe to join the community. Coupled with the difficulty in determining the attribution of a cyberspace user's actions, the cyber domain remains an environment that is contested in ways the terrestrial domains are not. The services' networks are under attack every day.

---

[51] Maj Adam Bixler in a personal interview on March 29, 2012.
[52] Col Robert Morris in a personal interview on February 24, 2012.
[53] Ellen Nakashima, *The Washington Post,* "Cyberattacks Should Require Presidential Authorization, Official Says," March 27, 2012.
[54] Col Robert Morris in a personal interview on February 24, 2012.
[55] Joseph S. Nye, Jr., *The Future of Power*, 126-127.

Based on each of the services' dependence on superiority in the cyber domain and challenges in achieving/maintaining superiority, three conclusions are drawn from the current modus operandi.

First, there are not enough trained cyber professionals in the USAF and (potentially) the DoD.[56] Improvements in technology encourage the assumption that power should be consolidated. In the cyber career fields this translates to restricting permissions and reducing workforce overhead in the general populous. The perception is that the "select few" and "golden children" are whisked-away for elitist training behind the doors of Top Secret vaults and "Green Doors."[57] The result is a significantly smaller force that does not interact with the rest of the service. Although the new cyber operations career field is too new for historical study, the risk of operating in a closed-off culture is that the experts will never leave the vaults and become further isolated and increasingly disconnected from the service it supports. More importantly, the community becomes detached from the senior leaders and decision makers in the service.

At a time when it is even more important for the cyber operators to become integrated with the services, the community appears to be distancing itself. There are two great risks with self-induced retrenchment. The first is that the leaders and services at-large become distrustful of cyber power and its potential applications. It has often been said, the cyber domain and the people associated with it look very much like the space domain and its' community twenty years ago. As highlighted in the last chapter, the space community is working to become more integrated in operations but because of the secrecy involved, many still dismiss space options at the expense of efficiency

---

[56] Lt Col Jason Sutton in a personal interview regarding USAF manpower and training. A deeper study of each of the services is required to determine if there is a shortage of trained cyber operators.

[57] "Green Doors" is a reference to jobs traditionally not available to the average worker. People do not apply for these jobs, rather people receive these assignments by way of a cryptic phone call from someone they have never heard of.

and increased risk. Without subject matter experts fully integrated into the peace and wartime planning staffs, leaders are less likely to call for cyber effects.

Accepting greater risk is the second byproduct of becoming disconnected. If the warfighters and senior leaders do not know what cyber can bring to the fight, they are less like to know how to ask for it. Or worse, the person in the seat will replace cyber effects with kinetic options. As seen in Bosnia and the AOC, due to a lack of confidence in space capabilities, increased risks to human life and military assets were repeatedly accepted over space courses of action. The answer is to grow the career field and integrated the subject matter experts into key positions and planning staffs.

The second conclusion to be drawn from the USCYBERCOM model and operations in the cyber domain is that there is confliction rhetoric of command and control. USCYBERCOM and the NSA appear to be the center of gravity for defending the GIG, but the reality is that the two organizations are dependent on the services to defend their own portions of the network. Further, USCYBERCOM's JOC is dependent on the services to push information for situational awareness. According to USSTRATCOM's fact sheet about USCYBERCOM, the subunified command is charged with "creating synergy that did not previously exist and synchronizing war-fighting effects to defend the information security environment."[58] While the command is able to pull together resources in reaction to unforeseen events, the deliberate planning process and dependency for the services to police themselves in handling the daily operations and defense of their portions of the GIG does not reflect the expectations of "synergy" and "synchronizing." Nor does it fully answer

[58] *US Cyber Command Fact Sheet*, December 2011 (retrieved from http://www.stratcom.mil/factsheets/Cyber_Command/ on March 19, 2012).

the Secretary of Defense's call for the "*integration* of cyberspace operations."[59]

Along the same lines, the lack of an Executive Agency assigned to one of the Armed Services presents a dilemma in standardizing defensive operations. USCYBERCOM is available to provide advice but expects the services to defend their own networks. The expectation could not be more plainly obvious than in General Alexander's admission that his command cannot defend the GIG.[60] Without one of the services taking the lead on tactics, techniques, and ensuring compliance with directives, the four services are all likely to develop their own procedures. Although large benefits can come from exploring such freedom, the services are missing an opportunity to collaborate and create synergies. Further, since the domain is manmade, by acting independently the services are also missing an opportunity to reengineer the domain in a way that could make it collectively stronger and more defensible.

The final conclusion to be drawn is the disconnect in ownership of the domain. The procedure for planning and conducting CNA operations appears to work,[61] however, the immediate vulnerability and threat is in the inability to defend the network. Unlike the other domains, cyberspace is persistently and unremittingly under attack. Due to the low cost in entering the domain and the incessant barrage of attacks, the struggle for superiority is not a matter of gaining and maintaining, but rather repeatedly repelling and protecting. Defense of the system is each COCOM's real contested battle space. CENTCOM is the only COCOM with a full CSE, but they have limited power and act more as an intermediary to USCYBERCOM. General Alexander "likened it to seeing

---

[59] SecDef Memo, *Establishment of a Subordinate Unified US Cyber Command Under US Strategic Command for Military Cyberspace Operations*, June 23, 2009. Emphasis added by thesis author.

[60] Noah Shachtman, *Wired Magazine*, "Military Networks 'Not Defensible,' Says General Who Defends Them," January 12, 2012.

[61] Due to security classifications and time constraints in writing this thesis, it was not possible to perform a historical evaluation of the effectiveness of the ITO process.

a cyber-intrusion happen at 'network speed' and then 'trying to send a regular mail letter to them [saying] that you're being attacked.'"[62] The CSE office more closely resembles the function of the JSpOC, except the barriers of entry and challenges to defending the systems are considerably different. It is also imperative to remember that only one COCOM has the fully established CSE office, while (presumably) all the COCOMs networks are attacked daily.

The COCOMs thus find themselves in a conundrum of being completely reliant on the cyber domain to conduct operations, but no authority or capability to defend it. Contributing to the dilemma, not having a service as the Executive Agency for cyberspace results in different tactics and procedures for handling the same types of attacks across multiple COCOMs. A tactic used to attack a US Navy-defended network in one AOR may be replicated in another AOR defended by the USAF. Additionally, the DoD tends to discriminate between COCOMs fighting in wars and ones that are operating from a peacetime organize, train, and equip posture. The reporting procedures and ownership of the processes for handling defense issues is different. Attacks against a USAF network in CENTCOM are handled through the CSE, USCYBERCOM, and a unit designated by USCYBERCOM. Attacks against a USAF network in Pacific Command (PACOM) are handled through INOSC-West and AFCERT.

Numerous lessons and recommendations surface from studying USCYBERCOM's ability to command and control the cyber domain. In addition, data points selected from the AOC and JSpOC models offer insight into ways of assuring superiority in cyberspace. The key to winning the fight in the cyber domain is to find the right model for command and control, growing the community, and placing the right

---

[62] Ellen Nakashima, *The Washington Post,* "Cyberattacks Should Require Presidential Authorization, Official Says," March 27, 2012. General Alexander was actually referring to the NSA observing a defense contractor being hit and gigabytes of information being stolen, but the principle theme remains the same.

permissions at the right levels. Only then can the DoD's most contested domain be secure. Today, and in the future, leveraging cyber superiority will be the key to remaining relevant in all the other realms.

Chapter 4
Constructing the Hybrid Model

For 53 years, not one American soldier has died as a result of enemy aircraft fire. I aim to extend this hard-earned dominance for another 53 years and more, and use cyber and space power to do it.
-- Secretary of the Air Force Michael W. Wynne

The linkages between an AOC, the JSpOC, and USCYBERCOM may not be immediately recognizable, but the three come together to form an effective bridge between the political will of the United States and its ability to influence world events. Seemingly the three models have many differences, but specific attributes led to their selection. The command and control structures represent the current models for supporting today's JFC through limited assets with increasing range and speed. The AOC enables control of airborne assets and retains the authority to employ them. Similarly, the JSpOC facilitates control of the space assets and the authority to utilize them. Finally, USCYBERCOM preserves control of the cyber forces and the authority to direct them. In all three models, there are restrictions and limits as to how the assets are used, but in general the authorities reside with the JFACC, the Commander of JFCC-Space, and the Commander of USCYBERCOM, respectively.

The three models have similar tasking and planning cycles, but very different command and control architectures in place. This final chapter will pull common threads together to evaluate whether the current USCYBERCOM model will be relevant in the future. Further, applicable data points from the air and space models are included in recommendations to ensure secure and reliable cyberspace operations in the future. Before beginning the evaluation, it is important to recognize the finer points of command and control in cyberspace.

Command and control in the air, sea, land, and space domains are dictated by ownership of the asset and permission to use them. The owning COCOM accepts responsibility for appropriately utilizing the assets for offensive purposes and also in defending them. Within the cyberspace domain, command, control, and ownership discourse go beyond offense and defense. It is also about access. There are two paradigms about allowing access and accepting risk in the cyber domain. The concern over granting access speaks to the often quoted parable, "risk accepted by one is risk accepted by all." Translated for the global cyber domain, risk accepted by a user in one location, falls on all the users on the network. The two methodologies for allowing access are found in closed- and open-systems.

Attaining Access: Closed-Systems and Open-Systems

The advocates for a centralized command and control structure traditionally follow a Clarke-like philosophy of a closed-system.[1] In a closed-system, a very small group of people have the decision making authority and a significantly reduced number of people have access at all. There are several benefits. First, this supports the philosophy of being able to see the broader landscape and promotes the idea of thorough interrogation and analysis of information; thus ensuring the end product is the best possible synthesis of all the parts. The final decision maker becomes the nerve center of all the data and is in the best possible position to make a decision for the entire system. A closed-system best represents how USCYBERCOM operates. In its current configuration, the headquarters at Fort Meade authorizes actions. For example, to request or employ cyber effects, the JFC works through the COCOM CSEs and the USCYBERCOM JOC.

Another benefit of the closed system is the reduced number of vulnerabilities. According to Martin Libicki, the DoD gravitates to closed

[1] Richard Clarke is a leading advocate for closed-systems and centralized control of cyberspace.

systems to become more "impervious" and ensure the system's security.[2] A closed system reduces access points, thereby reducing the number of possible locations to breach the system. Due to the proximity and small number of people in the system, it is also easier to enforce the rules, avert breaches in security, implement new policies, and monitor activities; thereby mitigating some risks. The heart of this rationale goes back to the dictum about who is accepting risk for whom. Assuming proper training and compliance with procedures, it is logical that constricting the number of people who can introduce risk constricts the opportunity of introducing risk. In this way, a tight knitting of individual wire strands produces a stronger cable than a loose collection of disparate lines.

A third advantage for operating in a closed system is that it can focus the forces. Placing responsibility for cyberspace in a centralized organization concentrates the efforts of the force. The organization becomes committed in every thought, action, and decision contributing to superiority in cyberspace.[3] Without distractions of competing priorities, the organization harnesses the intellect of all the employees and reaps the synergies. With so many undefined characteristics in cyberspace (e.g. "what constitutes an attack?") it is understandable why leaders want to restrict actions until the lexicon and procedures are articulated. The down side is that leadership models with high centralization have a tendency for high decision thresholds that require "larger and more continuous information flow."[4]

---

[2] Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (New York, NY: Cambridge University Press, 2007), 69.
[3] Antoine Bousquet, *The Scientific War of Warfare: Order and Chaos on the Battlefields of Modernity*, (New York, NY: Columbia University Press, 2009), 123.
[4] Martin van Creveld, *Command in War* (Cambridge, MA: Harvard University Press, 1985), 236.

Another advocacy argument for centralizing command and control of cyberspace relates to "techniques"[5] and collateral effects. Zero day vulnerabilities and techniques for protecting, attacking, and exploiting vulnerabilities in cyberspace are national treasures. Offensively, operations carelessly conducted or techniques frivolously wasted against enemies can lead to "holes" being patched, whereby the techniques cannot be used again. By constricting the span of control, more educated risk and value assessments are made before conducting operations. Seeing the bigger picture also minimizes mistakes that bleed into unintended areas or taking imprudent actions.[6] After all, not all targets are worth using the only silver bullet.

Finally, as with all actions in war, there are risks of unintended consequences and collateral damage. It is very difficult to positively map all integrated networks and systems, and it is possible to accidentally disable or disrupt unapproved targets, or unintentionally cause spillover effects into other areas.[7] If the actions are linked back to the DoD, the appropriate level of oversight and leadership needs to be in-place to mitigate taking risky actions that uncontrollably ripple through cyberspace.

Despite the arguments for a centralized command and control structure for cyberspace, there are equally convincing arguments that the information age demands a decentralized structure. Deeply-rooted, large hierarchical structures like the military are often times slow to move. Additive levels of leadership and organizational cooperation are not conducive to timely decision making. Libicki and van Creveld

---

[5] The word "techniques" refers to processes and procedures to defend, attack, and exploit in the cyber domain.
[6] Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to do About It* (New York, NY: Harper Collins Publishers, 2010), 211-212.
[7] Martin Libicki, *Conquest in Cyberspace*, 259.

present a more open and power distributed philosophy for command and control of cyberspace.[8]

The information age in general, and attacks through cyberspace, are not compatible with traditional visions of trenches, demilitarized zones, and battlefield lines. Just as airpower circumvented geographical boundaries and timetables, the speed and reach in cyberspace shatters all other mundane obstacles. Today, global reach attains new efficiencies as attacks are measured by the speed of light and the immense geographical spread of targets. Advantages from the processing power of computers enables the dissemination of responsibilities to lower echelons, and allows the information to reach the decision makers faster. Dispersing capabilities can build a layered system and mitigate the risk of a "recognisable head that can be decapitated."[9] The danger, however, in decentralizing control is that security risks can increase. David Lonsdale articulates this trade-off when discussing Just-In-Time technologies; it "allows a greater exploration of efficiencies, but at the same time creates a certain amount of fragility within the system."[10]

In today's military, the warfighter often operates farther outside the safe zones, and therefore deserves the tools and permissions required to fight the enemy (within reason). As difficult as it is to fight the enemy, it is also difficult to determine the thresholds of control in delegating control to the warfighter. By centralizing the capabilities of cyberspace in USCYBERCOM, the effects the warfighting leadership is permitted to leverage in cyberspace are delayed and possibly diminished. Instead, the JFC is put into a position of losing time with "Mother, may I?" (or more accurately "Mother, will you?") requests. Additionally, with the speed at which the battlefield can change (regardless of domain), the commander

---

[8] Libicki and van Creveld are leading advocates for open systems and decentralized control of cyberspace.
[9] David J. Lonsdale, *The Nature of War in the Information Age: Clausewitzian Future* (New York, NY: Frank Cass, 2004), 9.
[10] David J. Lonsdale, *The Nature of War in the Information Age*, 11.

executing the war needs the most accurate and relevant information. Centralized command and control systems are best suited for "high-intensity wars in homogeneous environments."[11] The battlefields of today and tomorrow will not to fit that description, and the warfighter needs a streamlined approach to defending and fighting from cyberspace.

When describing the attributes of the ideal command system, van Creveld portrays a system that is able to "gather information accurately, continuously, comprehensively, selectively, and fast."[12] Often the JFC is forced to make timely decisions, especially in regards to the inherent right to self-defense. The commander may not have time to wait for information still being analyzed and routed by a rear echelon force that is unaware of battlefield implications, changing circumstances, and fleeting opportunities. The information and capabilities need to be judicious and unimpeded. In the right construct, cyberspace could be a force multiplier. In the wrong construct, it could jeopardize operations.[13]

Potentially the greatest benefit of decentralized control of cyberspace is the ability to flex with conditions, which enables the discovery and creation of new techniques and defenses. Responsive and flexible networks need to match rapidly changing conditions, and decentralized systems are more equipped than centralized ones at managing an unpredictable environment.[14] In cyberspace, the ability to counter attacks and respond to battlefield inputs is dependent upon an adaptable environment. While hierarchal systems exist to gather information and provide predictability, decentralized systems are better at thriving on chaotic and unpredictable conditions.[15]

A byproduct of creating a construct that is responsive to changing conditions is new discovery. Technological superiority in cyberspace is a

---

[11] Antoine Bousquet, *The Scientific War of Warfare*, 160.
[12] Martin van Creveld, *Command in War,* 8.
[13] Martin van Creveld, *Command in War,* 8 & 171.
[14] Antoine Bousquet, *The Scientific War of Warfare*, 182.
[15] Antoine Bousquet, *The Scientific War of Warfare*, 181-182 & 205.

fleeting notion.[16] Many of the techniques for attack, defense, and espionage are countered by software programs constantly being upgraded, replaced, and hidden behind stronger firewalls and encryption measures. Placing cyber warriors outside the headquarters and empowering them to take action increases the opportunities of new discovery.

Seemingly, the structure that proposes the biggest pay-offs also incurs the most risk. The chances of finding new vulnerabilities are greater through decentralized command and control. Striking the perfect balance is the key to the symbiotic relationship command and control shares with access. The remaining section will strive to uncover that balance.

Comparing the AOC, JSpOC, and USCYBERCOM

The three models provide distinct constructs for command and control. For this study, the actual commanding and controlling was broken down into offensive and defensive actions, and then further broken down into three categories for measurement. Measuring the three important categories resulted in a positive (yes) or negative (no) outcome for each. The categories were used to determine the JFC's ownership of targets, assets, and authority.

In the offensive portion, the intent was to discern whether the JFC owned the enemy targets, the assets to strike the targets, and the authority to use the assets to attack the enemy targets. In the defensive portion, the goal was to determine if the JFC owned the targets, as well as command and control over the assets to defend them and, lastly, the authority to use them.

The AOC Model

The JFC utilizes an AOC model to conduct air operations for attaining wartime and contingency objectives. A chart was prepared to

---

[16] Martin van Creveld, *Command in War*, 231.

illustrate the amount of control the JFC possesses for conducting operations (Figure 11).

DOMAIN	C2 MODEL	ACTION	METHOD	RESPONSIBILITY	OWNERSHIP	TARGET	ASSET	AUTHORITY
AIR	AOC	OFFENSE	ATO TASKED	AOC	JFC OWNS	YES	YES	YES
		DEFENSE	AOC COD	AOC	JFC OWNS	YES	YES	YES

Figure 11: AOC Command and Control Model
Source: Author's Original Work

As discussed, the command and control model is broken into offensive and defensive operations. In the offensive portion, the method for tasking the aircraft is the 24-hour ATO, produced by the AOC's Combat Plans Division. The AOC is responsible for ensuring execution of the ATO and redirecting assets as required to handle dynamic targets and unforeseen circumstances. The four columns on the right of the chart depict the JFC's ownership of the enemy targets, the assets to hit the targets, and authority to strike the enemy targets (Figure 12, taken from Figure 11).

OWNERSHIP	TARGET	ASSET	AUTHORITY
JFC OWNS	YES	YES	YES

Figure 12: AOC Command and Control Breakdown
Source: Author's Original Work

In all three categories, the JFC possesses command and control of the offensive operations, as evidenced by the B-2 prosecuting targets in Kosovo. After crossing the Prime Meridian, the B-2s belonged to the JFC, who had the authority to hit the targets designated by the AOC staff (through the ATO or information relayed to conduct flexible targeting).

When evaluating the defensive portion of the model, it is easy to see that the JFC also possesses the appropriate command and control to protect the aircraft assigned (targeted by the enemy), and the assets and authority to protect them. For instance, in the event of a downed allied aircraft, the AOC would deploy the Combat Search and Rescue teams and support aircraft to secure the area.

When analyzing the JFC's ability to direct offensive and defensive operations with aircraft, the AOC is a useful model for command and control. Nonetheless, it is the ownership of the target selection, possession of the assets, and authority to leverage the two together that enables the JFC to fight and win the battles.

The JSpOC Model

The JFC normally delegates space responsibilities to the JFACC and the AOC, and DIRSPACEFOR handles the day to day operations. To request space effects, the DIRSPACEFOR – operating on behalf of the JFACC and JFC – coordinates requests with the JSpOC. The JSpOC Combat Plans Division then fills the requests by tasking units through the JSTO. As an example, the DIRSPACEFOR could submit a request for enhanced GPS capability in a region and the JSpOC would try to support the request by tasking the responsible Schriever Air Force Base unit for concentrated power.

As this scenario reflects, command and control responsibility for space assets and the authority to employ them remains with the commander JFCC-Space. The JFC owns the targets but not the satellite assets, nor the authority to task them. In the JSpOC model, the JFC's command and control authorities is colored green for the target column, and yellow for the asset possession and employment authority columns (Figure 13). The color yellow was chosen because it represents a mismatch between the JFC's *desire* to take action and the warfighter's *ability* to take action. Red would reflect a *need* to take action. The small number of DoD satellites was also taken into consideration, and the fact those numbers are not likely to grow. Therefore the last two columns are colored yellow instead of red.

DOMAIN	C2 MODEL	ACTION	METHOD	RESPONSIBILITY	OWNERSHIP	TARGET	ASSET	AUTHORITY
SPACE	JSpOC	OFFENSE	JSTO TASKED	JSpOC	JFC OWNS	YES (REQUESTED)	NO	NO
		DEFENSE	INDIVIDUAL UNITS	UNITS	JFC OWNS	NO	NO	NO

Figure 13: JSpOC Command and Control Model
Source: Author's Original Work

Considering a defensive scenario where the DoD satellites become targets, the JFC is not responsible for the satellites, the assets or procedures to protect them. The JFC also does not possess the authority to do anything about the attack. In this circumstance, the JFC is absolved of any actions and responsibility, and the chart is coded green across the board.

For space defense, the home units remain responsible to defend their own systems. In cases like this, the JSpOC maintains situational awareness and contact with the units controlling the platforms, but retains limited capability. If, for example, another object were to hit a GPS satellite (intentionally or unintentionally), the operators at Schriever Air Force Base are responsible for defending the platform.

The USCYBERCOM Model

In requesting cyberspace effects, the JFC utilizes COCOM CSEs to coordinate with USCYBERCOM. USCYBERCOM maintains control of operations, and the President is the authorizing authority for attacks.[17] COCOMs make requests for cyberspace effects by interjecting CyERFs into the 24-hour ITO production process. The battle rhythm for submitting requests and creating tasking orders is similar to the AOC's ATO cycle, but the ownership of targets, assets, and permissions more closely resembles the JSpOC model. Like the JSpOC model, the JFC owns the targets in the AOR but not the assets or authority to employ their effects. The assets capable of delivering the effects receive their

[17] Department of Defense Cyberspace Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934, November 2011, 5.

tasking through USCYBERCOM. In this way, USCYBERCOM exercises authority over the units through the ITO.

Based on the JFC's command and control authorities in the USCYBERCOM model, the target column is shaded green. As in the JSpOC model, the asset and authority columns would be yellow due to a combination of the assets residing outside the control of the JFC and the relatively small number of certified cyber operators in the DoD. Unlike the expense of developing and deploying additional space assets, however, the cyber community's expenses are minimal and for this reason the color coding is yellow but transitioning to red. The transition to red reflects the ability to grow the force down the road as well as the JFC's potential *needs* in the future. A final chart is included to illustrate the amount of control the JFC possesses for conducting cyber operations (Figure 14).

DOMAIN	C2 MODEL	ACTION	METHOD	RESPONSIBILITY	OWNERSHIP	TARGET	ASSET	AUTHORITY
CYBER	USCYBERCOM	OFFENSE	ITO TASKED	USCYBERCOM	JFC OWNS	YES (REQUESTED)	NO	NO
		DEFENSE	INDIVIDUAL SERVICES	UNITS	JFC OWNS	YES	NO	NO

Figure 14: USCYBERCOM Command and Control Model
Source: Author's Original Work

With regards to defensive actions in cyberspace, the actions taken to protect the GIG fall into two categories: proactive measures and reactive/self-defense measures. Although USCYBERCOM does assist with the proactive measures and issue IAVAs, the bulk of the defense falls on the individual service cyber commands to monitor and control. In the USAF's case, whether the request for defensive action trickles up through the INOSCs and CERT or through the CSEs to USCYBERCOM and a USAF unit, the service is responsible for its own defense. When considering what targets the JFC would be concerned with, they are the JFC's own networks and parts of the GIG that support or reside in the COCOM's AOR. For this reason, the targets belong to the JFC and are appropriately shaded green. Reflecting on the JSpOC illustration for

defense in space, the unit under attack has the assets and authority to take action. This is not the case in the cyberspace model. The JFC's command and control *is the target*, but the COCOM does not retain any assets or authority to defend itself. For this reason the blocks are colored red. Based on the inherent right to self-defense, pace of operations on the virtual and physical battlefield, and the volume of daily attacks, the JFC *needs* to be able to defend its own networks.

Together the three models present a visual image of the amount of command and control the warfighter wields under the current constructs, and is displayed in Figure 15.

DOMAIN	C2 MODEL	ACTION	METHOD	RESPONSIBILITY	OWNERSHIP	TARGET	ASSET	AUTHORITY
AIR	AOC	OFFENSE	ATO TASKED	AOC	JFC OWNS	YES	YES	YES
		DEFENSE	AOC COD	AOC	JFC OWNS	YES	YES	YES
SPACE	JSpOC	OFFENSE	JSTO TASKED	JSpOC	JFC OWNS	YES (REQUESTED)	NO	NO
		DEFENSE	INDIVIDUAL UNITS	UNITS	JFC OWNS	NO	NO	NO
CYBER	USCYBERCOM	OFFENSE	ITO TASKED	USCYBERCOM	JFC OWNS	YES (REQUESTED)	NO	NO
		DEFENSE	INDIVIDUAL SERVICES	UNITS	JFC OWNS	YES	NO	NO

Figure 15: Command and Control Comparison
Source: Author's Original Work

Constructing the Hybrid Model for Cyberspace

The challenge facing the [DoD] is therefore to harness the flexibility and adaptability of networks while preserving some hierarchical features – hybridization is the goal.

-- Antoine Bousquet

Having analyzed each of the three models and explored the command and control capabilities and restraints, modest changes to the cyber construct would enable the JFCs and USCYBERCOM to improve the performance of their missions. Putting control in terms of access, it

is helpful to understand how the DoD currently operates and what the recommended changes mean in these regards.

Today, the United States Government operationalizes cyberspace utilizing closed-system, centralized constructs for command and control. USCYBERCOM is the nerve center that funnels information and monitors inputs from the field. The command provides guidance and distributes information through the individual service components. As a vetting office and coordinator for the National Command Authority, the sub-unified command authorizes operations in cyberspace. Although USCYBERCOM permits the services to take action in subordinate roles, they do not relinquish authority to the warfighting commanders.

It is natural for a warfighter to covet all of the possible tools to do their job. It is also innate for someone under attack to desire the means to respond or retaliate; few things are more frustrating than being powerless and vulnerable. Of all the domains the DoD operates within and from, cyberspace is the most contested. There are two rubs with the current construct. First, the model differentiates between at-war COCOMs and peacetime COCOMs, regardless of the fact both are constantly under a barrage of attacks. Presuming the levels and types of attacks are not different, separating response scenarios and processes defies logic. Both should be treated the same. An attack against one is likely the same attack against another. The second point of contention is that under the current construct, USCYBERCOM is unable to defend the GIG. The model must reflect the ability to preserve the GIG and ensure the relevance of the domains that rely upon it.

The first change in the new cyberspace model is to establish a permanent joint-command and control office in each geographic COCOM for cyber operations. The new office will be responsible for providing cyber superiority to all the services in the region, whether the AOR is at peace or war. The virtual world is never at rest and neither should the common protection of it.

The establishment of six Global Information Grid Combatant Command Cyber Centers, or GIG-C4, (GIG-AFRICYBER, GIG-CENTCYBER, GIG-EUCYBER, GIG-NORTHCYBER, GIG-PACYBER, and GIG-SOUTHCYBER) will provide common offices for all the services to work with, and will replace *some* of their current service-parochial operations centers.[18] Instead of breaking the GIG into four parts for each of the services to manage, the model will break the GIG into six parts for the COCOMs to manage on behalf of all the services. The biggest difference being that the services come together to defend by geographic location, as opposed to distributing responsibility and defending by geographic location within each service.

The GIG-C4s will operate 24/7, produce their own ITOs, provide command and control for the geographic commander, and reachback capability for all the services in the AOR. Shifting the ability to take action to the COCOM solves two critical problems identified by the United States Government Accountability Office (GAO), in their 2011 report. First, it addresses the problem of COCOMs not aware of cyberspace problems in their AOR and their inability to take action or prepare for the future.[19] The delegation of authority and redistribution of forces also answers the gaps identified by COCOMs and USSTRATCOM in growing and integrating cyber forces into operations, "particularly for full-spectrum cyberspace operations."[20]

In the new model, the relationship with USCYBERCOM would resemble the same type of relationship the services have with the Joint Staff. USCYBERCOM remains a vital model for coordinating efforts, contingency and long term planning, large offensive attacks requiring Presidential approval, mediating to shape cyberspace, and executing

---

[18] A deliberate study needs to occur for looking at the benefits and risks of standing up a GIG-SOCYBER.
[19] GAO-11-75, *Defense Department Cyber Efforts: DoD Faces Challenges in its Cyber Activities*, July 2011, 7.
[20] GAO-11-75, *Defense Department Cyber Efforts*, 38.

special operations. The new image and delineation of responsibilities solves two overarching problems. First, in the current model, there are cases of confusion when command and control falls between (or on both) service responsibility and COCOM authority.[21] ". . . the supporting relationships necessary to achieve command and control of cyber operations remain unclear. According to the *National Military Strategy for Cyberspace Operations*, the United States can achieve superiority in cyberspace only if command and control relationships are clearly defined and executed."[22] The second problem comes from concerns about the commander of USCYBERCOM also wearing the hat of Director of the NSA. The fear is that USCYBERCOM will "become too focused on intelligence structures in detriment to a focus on operations in support of the combatant commands."[23] Establishing the GIG-C4s allays the concerns about the commander ensuring the success of one mission at the expense of another. The new model also allows USCYBERCOM to still influence and oversee operations. The link that will allow USCYBERCOM to remain tied-into the GIG-C4s comes through the creation of a new position.

A Director of Cyberspace Forces (DIRCYBERFOR) will lead each of the GIG-C4 offices and act as a principal advisor to the Geographic Combatant Commander (GCC). In this way, the DIRCYBERFOR fills the roll of the AOC's DIRSPACEFOR and the liaisons. The DIRCYBERFOR runs the day-to-day operations, synchronizes cyberspace effects throughout the AOR, and coordinates efforts that cannot be handled in-residence. Like the selection process for the DIRSPACEFOR, the DIRCYBERFOR will be a senior leader in the cyberspace career field and hand-selected for the assignment by the commander of USCYBERCOM. In addition to geographic responsibilities, the DIRCYBERFOR will tie the

---

[21] GAO-11-75, *Defense Department Cyber Efforts*, inside cover page.
[22] GAO-11-75, *Defense Department Cyber Efforts*, 6.
[23] GAO-11-75, *Defense Department Cyber Efforts*, 26.

GIG-C4 back into USCYBERCOM and the five sister units. In the event a JFC is activated in an AOR, the DIRCYBERFOR will also be the point of contact for JFCs that require cyberattack and defense (assuming the JFC is not the GCC).

The second change in the cyberspace model comes with the new hybrid structure; it entails decentralizing some permissions and responsibilities to the COCOMs. Looking at the offensive side of command and control, there is not a significant amount of change between the JFC's responsibilities in the current USCYBERCOM model and the JSpOC model. The JFC owns the targets and requests support, and the supporting command has the authority and responsibility to try and provide assets. The goal of the new model will be to move GIG-C4's offensive capabilities to in-between the AOC and JSpOC models.

As the experience of cyber operators grow, some authorities and assets need to be pushed to the COCOMs to conduct operations for the JFC. Parameters and rules of engagement need to be developed, and some degree of oversight required, but it is narrow-minded to believe *all* attack options will *always* exist with the President. Every day young pilots are trusted with kinetic capabilities that immediately terminate life and destroy property. As the DoD's cyber forces mature, the permissions delegated and the risks accepted must grow. Placing parameters on the capabilities of COCOM cyber operators is no different from placing rules of engagement on the kinetic warriors. With the increase reliance and vulnerability to cyber warfare, it is unrealistic to imagine the President can retain exclusive control of cyberattack. The line between active-defense and offense blurs more every day, and actions resulting in tactical level impacts need to be decentralized. This is what Maj Gen Suzanne Vautrinot was referring to when describing cyber defense. "It's like a hospital gown. You're covered in the front, but hanging out in the

back. We need to get proactive in how you use the defensive structure."[24]

For the defensive side of GIG-C4, the objective is to enable the COCOMs to defend themselves. The centers for each COCOM will handle attacks regardless of whether the AOR is involved with a kinetic war or not. Compared to how the USAF currently operates, in the new capacity the GIG-C4 replaces and merges the two disparate processes of either working through an INOSC or through a CSE. In this way, the GIG-C4 will move towards an AOC type ownership of the assets and authority. Figure 16 depicts the changes as command and control moves from the USCYBERCOM model to the GIG-C4 model.

DOMAIN	C2 MODEL	ACTION	METHOD	RESPONSIBILITY	OWNERSHIP	TARGET	ASSET	AUTHORITY
CYBER	USCYBERCOM	OFFENSE	ITO TASKED	USCYBERCOM	JFC OWNS	YES (REQUESTED)	NO	NO
		DEFENSE	INDIVIDUAL SERVICES	UNITS	JFC OWNS	YES	NO	NO

DOMAIN	C2 MODEL	ACTION	METHOD	RESPONSIBILITY	OWNERSHIP	TARGET	ASSET	AUTHORITY
CYBER	GIG-C4	OFFENSE	ITO TASKED	COCOM / USCYBERCOM	JFC OWNS	SOME TIMES	SOME TIMES	SOME TIMES
		DEFENSE	COCOM	COCOM	JFC OWNS	YES	YES	YES

Figure 16: Cyberspace Model: Before and After
Source: Author's Original Work

There are several benefits to implementing the GIG-C4 model. First, it forces the services to cooperate and coordinate in bringing their systems in line with each other. Considering there are 7 million devices spread across 15,000 networks, there are a considerable number of potential vulnerabilities in the GIG.[25] Aligning the services together and merging/eliminating networks is the first step in rebuilding the GIG, reducing vulnerabilities, and developing joint tools, techniques, and procedures. As a man-made domain, deliberately shaping the GIG can

[24] Amy McCullough, "Don't Let it All Hang Out," *Air Force Magazine*, March 26, 2012.
[25] *New York Times*, "Attacks on Military Computers Cited", April 15, 2010 (retrieved from http://www.nytimes.com/2010/04/16/world/americas/16military.html on March 20, 2012 and Referenced in Joseph S. Nye, Jr's book *The Future of Power*, 132.)

provide more interoperability and fewer liabilities to the system.[26] Considering cyberspace is the most contested domain and that the commander of USCYBERCOM admits the command is unable to defend it now is the time to take action and harness synergies gained from merging the talents of all the services.

Another benefit is that the new model mitigates some of the risk in a centralized construct becoming a self-perpetuating information gathering organization, and losing the ability to see the big picture. "The greater problem with centralization is one of limited attention. Attention is often called the only persistent scarcity in the information age."[27] An organization like that cannot satisfy its own need for information, so the gathering of information becomes an end of its own, and despite the quality of the information there is just too much of it to be actionable.

Decentralizing also minimizes some of the risks incurred in becoming entrenched. Although there is great internal collaboration amongst highly specialized teams, USCYBERCOM can become stovepiped and myopic. This is the first step in becoming obsolete. It also assumes that the organization actually has all the intellectual property required to meet the tasks. Regardless, the parts of the organization can become so specialized in thinking and skillsets that "the less capable any of them separately is of making independent decisions that may affect the whole, and the greater the need for overall direction from the top."[28] Allowing some decentralization allows the force to grow in numbers and perspective, and opens the aperture in seeing the threats and possibilities in the environment.

---

[26] Maj Gen Brett T. Williams, "Ten Propositions Regarding Cyberspace Operations," *JFQ,* Issue 61, 2d Quarter 2011, 14.
[27] Josef Falkinger, "Limited Attention as a Scarce Resource in Information-Rich Economies," *The Economic Journal*, Issue 118, October 2008 and Referenced in Martin Libicki's book, *Conquest in Cyberspace: National Security and Information Warfare* (New York, NY: Cambridge University Press, 2007), 110.
[28] Martin van Creveld, *Command in War,* 236.

A significant requirement in developing the GIG-C4 construct is to increase the size, awareness, and interoperability of the cyberspace community. The GIG's defense is strengthened by creating experts who understand threats and tactics within each of the AORs. Although attacks can originate from outside an AOR, it is logical that the actors with the greatest interests in interfering with military operations are from the countries in that COCOM's region. The regional GIG-C4 teams can also build relationships and understanding with the supported bases and their missions. For attacks that originate outside the AOR, the impacted COCOM GIG-C4 can coordinate appropriate responses with USCYBERCOM, and leverage capabilities and responsibilities residing in other GIG-C4s.

By growing the cyber force through the GIG-C4s, the senior leaders are provided a better opportunity to take a more active role in the cyber domain. Doing so helps build trust and understanding in how to leverage cyber effects and integrate them into the operational environment. The DIRCYBERFOR is key to providing subject matter expert advice to the commander and successfully operationalizing the domain in the COCOM. Despite significant efforts, growing dependency, and decades of integration, space is still struggling with building trust in the warfighter. Cyberspace is even farther behind.

Finally, by methodically decentralizing small amounts of control at a time, the GIG-C4s can succeed. The key is to build a plan that competently grows the forces and links that growth to a laddered approach of decentralizing command and control. Defense of the networks need to be the first priority. Due to the vast military reliance on cyberspace, a strong defense is a prerequisite to building an offensive capability. USCYBERCOM needs to establish incremental permissions, access, and responsibilities and link them to benchmarks. As the GIG-C4s stand-up, they will be authorized specific capabilities based on being at the bottom rung of a ladder. When the cyber centers meet certain

criteria they can move to the next rung and next set of responsibilities. Each step on the ladder incrementally moves the model to a more open-system, until the COCOMs have full responsibility for defending their networks. The offensive piece will likely need to follow much farther down the road as confidence in the cyber community grows and the National Command Authority delegates responsibilities for specific actions.

Despite the many reasons to establish the GIG-C4 model, there are three drawbacks to decentralizing some of the command and control responsibilities. Recognizing the drawbacks upfront is the key to overcoming them. First, the cyber community has already spent several years in flux. A number of units, joint task forces, and organizations have been stood-up and stood back down. Implementing another large change has cascading effects on the warfighting as well as the train-and-equip missions. Each of the services already faces challenges with defending their parts of the GIG and keeping their networks operational, without forcing a merger of systems and programs. The GIG began as a way of sharing information in an academic environment and with each passing day a deliberate attempt to reshape it will only make the network that much harder to eventually rewire. As the DoD grows in dependence of the cyber domain, and as warfare moves more towards inclusion of cyberspace attacks, the vulnerabilities in the system will become more costly later on. The time to take action has already arrived.

The second negative aspect is that moving towards a more open system introduces more risk. Allowing more users in the system will likely increase the number of mistakes. Although it is desirable to have a bridge supported by premium cables of the finest wire strands, it is important to remember there are hundreds of other cables carrying some of the weight. The good news is that mistakes made will likely *not* cause loss of life or destruction of property. In the kinetic world, mistakes can cost pilots their lives or cause grave harm to innocent civilians, such as

in the unfortunate bombing of the Chinese Embassy during OAF.[29] Worst case scenarios always deserve attention and contingency planning, but restricting capability and growth at the expense of unlikely doomsday scenarios is more reckless than attempting to set the right conditions.

Finally, the last drawback to moving from the USCYBERCOM model to a geographically centric model is that the cyberspace domain is not geographically centric. Although it complicates matters to think about geography in cyberspace, it also provides a mechanism for preventing the force from spinning in all directions. Attribution is a hard task in cyberspace and the linkages and routes circumnavigate physical fiefdoms. The chances of finding issues that originate from another GIG-C4's AOR are likely. Procedures and relationships must be established to allow the transfer of authority and information between GIG-C4s. Formalizing procedures for passing information that bleeds-over from one territory to another will help ensure the networks remain operational.

Growing the Cyberspace Force

The intent of this thesis is to concentrate on the command and control model. Throughout the research, however, a theme about the size of the cyber community continued to grow. The real assets in the cyber domain are the people, not the hardware. This is a paradigm shift from the perception of assets in the other domains.[30]

With the AOC model, the assets are the B-2s. The B-2s are a very small fleet of 20 operational aircraft that travel at subsonic speeds, and are only able to employ munitions wherever they are at in the world. In the JSpOC model, the assets are the 54 DoD satellites. Their strength is

---

[29] Chicago Tribune, *Chinese Embassy Shattered by Blast*, May 8, 1999 (retrieved from http://articles.chicagotribune.com/1999-05-08/news/9905080069_1_embassy-attack-cluster-bombs-nato-bomb on April 4, 2012).

[30] Thomas Kuhn, *The Structure of Scientific Revolutions* (Chicago, IL: The University of Chicago Press, 1996), 7.

that they are always deployed and the constellations enable near real-time delivery of effects. Because of the limited number of B-2s and satellites, expense in deploying more assets, and the global utility, the command and control permissions will likely not change.

In the USCYBERCOM model, on the other hand, the assets are the cyber operators. The operators need physical hardware, connectivity, and techniques, but the expense of those items is minimal compared to B-2s and satellites. There is unlimited potential to how many cyber operators the DoD can create. The fact that operators deliver effects at the speed of light from virtually anywhere in the world magnifies the importance of forming a strong corps of cyberspace operators. USSTRATCOM identified that the cyber force is "undersized and unprepared to meet the current threat, which is projected to increase significantly over time."[31] Additionally, the Joint Staff identified four capability-gaps resulting from the size of the force, and COCOMs identified shortages in trained cyber operators.[32] Further studies need to be conducted to determine the proper size of the cyberspace community.

Conclusion

The thesis started with an analogy of a suspension bridge. Expanding the picture of the suspension bridge allows one to see that there are multiple towers (Figure 17). Each tower represents a separate COCOM, and the GCC's span of control is measured between the points where the suspender cable comes in contact with the main deck. Airmen, Soldiers, Sailors, and Marines transfer from the control of one JFC to another as they enter their span of control. The locations are finite, but the cyberspace element is continuous and USCYBERCOM's presence flows throughout the bridge. By moving from the USCYBERCOM model of command and control to the GIG-C4 model, the suspension cables connecting the suspender cable to the deck come

[31] GAO-11-75, *Defense Department Cyber Efforts*, inside cover page.
[32] GAO-11-75, *Defense Department Cyber Efforts*, 8.

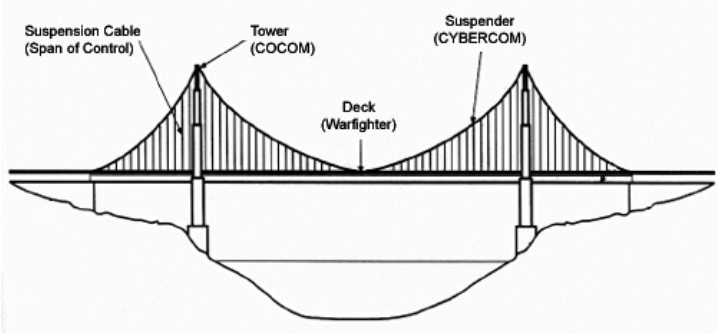

Figure 17: Suspension Bridge Diagram Complete
Source: Adapted from
http://mmem.spschools.org/grade3science/3.bldg/Suspension.html

alive. This is where the JFCs exercise command and control of their portion of the GIG and integrate it into all of their resources. By having the assets and authority to leverage cyber capabilities, the JFCs are able to distribute strains that exist in the system. Just as each cable distributes a portion of the bridge's weight; it works as a part of a larger system. The distribution of power to the JFC allows the operational command to determine the amount of slack that needs to exist in the cables.

With each tower representing a COCOM warfighter, USCYBERCOM is still involved, acting as the main suspender cable that connects the towers and the GIG. The decentralized construct allows detailed focus within limited spans of control while also tempering the power and risks. By enabling the COCOMs to plan and control parts of all five of the domains (air, ground, sea, space, and cyber), the DoD can better leverage asymmetric advantages to fight for, secure, and protect America's interests. The COCOM's authorization to manage a geographic AOR must extend to the terrestrial and cyber domains, thus allowing the planners and warfighters to continue to develop the most effective and efficient strategies for protecting and exploiting strengths and targeting weaknesses in their regions.

Cyberspace is a new tool to fight with, and enables instruments of power within the other domains. The cyber domain cannot be completely

controlled, but decentralization of some aspects of cyberspace will better prepare the DoD to leverage all five domains. The system will be more resilient and adaptive to conditions that can change the battlefield at the speed of light. Only through decentralized control can the DoD understand how to bridge the gaps in and between cyberspace and war, and maximize the conditions for this element of warfighting.

Abbreviations

ADCON	Administrative Control
AFCENT	Air Forces Central
AFCYBER	Air Forces Cyber
AFDD	Air Force Doctrine Document
AOC	Air Operations Center
AOD	Air Operations Directive
AOR	Area of Responsibility
ATO	Air Tasking Order
CERT	Computer Emergency Response Team
CNA	Computer Network Attack
CND	Computer Network Defense
CNE	Computer Network Exploitation
COA	Course of Action
COCOM	Combatant Command
COD	Combat Operations Division
CONUS	Continental United States
CPD	Combat Plans Division
CSE	Cyber Support Element
CyERF	Cyber Effect Request Form
DIRLAUTH	Direct Liaison Authority
DIRSPACEFOR	Director of Space Forces
DoD	Department of Defense
GAO	Government Accountability Office
GIG	Global Information Grid
GIG-C4	Global Information Grid Combatant Command Cyber Center
GPS	Global Positioning System
INOSC	Integrated Network Operations Security Center
IAVA	Information Assurance Vulnerability Alert
ISR	Intelligence, Surveillance, and Reconnaissance
ITO	Information Tasking Order
JAOP	Joint Air Operations Plan
JDAM	Joint Direct Attack Munition
JFACC	Joint Forces Air Component Commander
JFC	Joint Forces Commander
JFCC-Space	Joint Forces Component Commander - Space
JOC	Joint Operations Center
JP	Joint Publication
JSpOC	Joint Space Operations Center
JSOP	Joint Space Operations Plan
JSTO	Joint Space Tasking Order
LNO	Liaison Officer
MAAP	Master Air Attack Plan
MCAP	Master Cyber Attack Plan

MSP	Master Space Plan
NATO	North Atlantic Treaty Organization
NSA	National Security Agency
OAF	Operation Allied Force
OCONUS	Outside the Continental United States
OPCON	Operational Control
PACAF	Pacific Air Forces
PACOM	Pacific Command
PGM	Precision Guided Munitions
RAF	Royal Air Force
RFF	Request For Forces
SCA	Space Coordinating Authority
SOD	Space Operations Directive
TACON	Tactical Control
USAF	United States Air Force
USAFE	United States Air Forces Europe
USCYBERCOM	United States Cyber Command
USJFCOM	United States Joint Forces Command
USSTRATCOM	United States Strategic Command

Bibliography

Academic Paper

Hand, Maj Richard A. "Who Should Call the Shots? Resolving Friction in the Targeting Process." *School of Advanced Airpower Studies*, June 2001.

Hathaway, Col David C. "The Digital Kasserine Pass: The Battle Over Command and Control of DoD's Cyber Forces." *21st Century Defense Initiative Policy Paper at Brookings*, July 15, 2011.

Lamb, Lt Col Michael W. "Operation Allied Force: Golden Nuggets for Future Campaigns." *Air War College*, August 2002.

Smail, Lt Col John P. "Designed to Win: An Agile Approach to Air Force Command and Control of Cyberspace." *School of Advanced Air and Space Studies*, June 2010.

Articles

Air Force News. "Air Force Stands Up First Network Warfare Wing." July 5, 2006.

Associated Press and MSNBC. "US Eyes N. Korea for 'Massive' Cyber Attacks." Updated July 9, 2009, http://www.msnbc.msn.com/id/31789294/ns/technology_and_science-security (accessed December 29, 2011).

Atkinson, David. "B-2s Demonstrated Combat Efficiency Over Kosovo." *Defense Daily,* July 1, 1999.

Barnes, Ed. "North Korea's Cyber Army Gets Increasingly Sophisticated." *FoxNews.com*, May 17, 2011, http://www.foxnews.com/world/2011/05-17/north-koreas-cyber-army-gets-increasingly-sophisticated.html (accessed on December 29, 2011).

Chicago Tribune. "Chinese Embassy Shattered by Blast." May 8, 1999, http://articles.chicagotribune.com/1999-05-08/news/9905080069_1_embassy-attack-cluster-bombs-nato-bomb (accessed on April 4, 2012).

Claburn, Thomas. "Cyber Attack Code Starts Killing Infected PCs." *Information Week*, July 10, 2009, http://www.informationweek.com/news/government/security/218401559 (accessed December 29, 2011).

Cobb, Lt John. "Centralized Execution, Decentralized Chaos: How the Air Force is Poised to Lose a Cyber War." *Airpower Journal*, Summer 2011.

Dolman, Everett C. "New Frontiers, Old Realities." *Strategic Strategies Quarterly*, Spring 2012.

Falkinger, Josef. "Limited Attention as a Scarce Resource in Information-Rich Economies." *The Economic Journal*, Issue 118, October 2008

Grant, Rebecca. "The Afghan Air War." *Air Force Association Special Report*, September 2002.

Grant, Rebecca. "Victory in Cyberspace." *Air Force Association Special Report*, October 2007.

Grier, Peter. "The Investment in Space," *Air Force Magazine*, February 2000, http://www.airforce-magazine.com/MagazineArchive/Pages/2000/February%202000/0200investment.aspx (accessed March 7, 2012).

Hinote, Lt Col Clint. "Centralized Control and Decentralized Execution: A Catchphrase in Crisis?" *Air Force Research Institute Papers* . Maxwell AFB, AL: Air University, Air Force Research Institute, March 2009.

Hollis, Lt Col David M. "USCYBERCOM: The Need for a Combatant Command versus a Subunified Command." *JFQ,* Issue 58, 3rd Quarter 2010.

McCullough, Amy. "Don't Let it All Hang Out." *Air Force Magazine*, March 26, 2012.

Nakashima, Ellen. "Cyberattacks Should Require Presidential Authorization, Official Says." *The Washington Post,* March 27, 2012.

Nelan, Bruce W. "Into the Fire." *Time Magazine,* April 5, 1999, www.ebscohost.com (accessed on January 27, 2012).

New York Times. "Attacks on Military Computers Cited." April 15, 2010, http://www.nytimes.com/2010/04/16/world/americas/16military.html (accessed March 20, 2012).

Rife, Shawn P. "Kasserine Pass and the Proper Application of Airpower." *Joint Forces Quarterly*, Autumn/Winter 1998-1999.

Sang-Hun, Choe and John Markoff. "Cyberattacks Jam Government and Commercial Web Sites in US and South Korea." *New York Times*, July 9, 2009, http://www.nytimes.com/2009/07/09/technology/09cyber.html?adxnnl=1&pagewanted=print (accessed on December 29, 2011).

Shachtman, Noah. "Military Networks 'Not Defensible,' Says General Who Defends Them." *Wired Magazine*, January 12, 2012.

Singer, P.W. "Double-hatting Around the Law: The Problem with Morphing Warrior, Spy and Civilian Roles." *Armed Forces Journal*, April 2012, http://www.armedforcesjournal.com/2010/06/4605658/ (accessed on May 12, 2012).

Tirpak, John A. "Victory in Kosovo." *Air Force Magazine*, July 1999.

Tirpak, John A. "With Stealth in the Balkans." *Air Force Magazine,* October 1999.

Williams, Maj Gen Brett T. "Ten Propositions Regarding Cyberspace Operations." *JFQ*, Issue 61, 2d Quarter 2011.

Williams, Maj Gen Brett T. "The Imperative for Shaping Cyberspace." *ITEA Journal 2010*, Issue 31: 439-441, December 2010.
Zweibelson, Ben. "Penny Packets Revisited: How the USAF Should Adapt to 21st Century Irregular Warfare." *Small Wars Journal*, September 29, 2010.

Books

Air Force Research Institute. *AU-18 Space Primer*. Maxwell AFB, AL: Air University Press, 2009.
Bousquet, Antoine. *The Scientific Way of Warfare: Order and Chaos On the Battlefields of Modernity*. Annapolis, MD: Columbia University Press, 2009.
Clarke, Richard A., and Robert K. Knake. *Cyber War: the Next Threat to National Security and What to Do About It*. Annapolis, MD: Ecco, 2010.
Clausewitz, Carl von. *On War*. Reprint ed. Annapolis, MD: Princeton University Press, 1989.
Corbett, Sir Julian Stafford. *Some Principles of Maritime Strategy*. Annapolis, MD: United States Naval Institute, 1988.
Creveld, Martin Van. *Command in War*. Annapolis, MD: Harvard University Press, 1987.
Demchak, Chris C. *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security*. Annapolis, MD: University of Georgia Press, 2011.
Edwards, Paul N. *The Closed World: Computers and the Politics of Discourse in Cold War America (Inside Technology)*. Annapolis, MD: The MIT Press, 1997.
Henriksen, Dag. *NATO's Gamble: Combining Diplomacy and Airpower in the Kosovo Crisis, 1998-1999*. Annapolis, MD: Naval Institute Press, 2007.
Hughes, Daniel J. *Moltke on the Art of War: Selected Writings*. New York, NY: Random House Ballantine Publishing, 1993.
Johnson-Freese, Joan. *Space as a Strategic Asset*. Baltimore, MD: Columbia University Press, 2007.
Keuhl, Daniel T. "From Cyberspace to Cyberpower: Defining the Problem" in Kramer, Franklin D., Stuart H. Starr, and Larry Wentz, eds. *Cyberpower and National Security*. Annapolis, MD: Potomac Books Inc, 2009.
Klein, John J. *Space Warfare: Strategy, Principles and Policy (Space Power and Politics)*. Baltimore, MD: Routledge, 2006.
Kramer, Franklin D., Stuart H. Starr, and Larry Wentz, eds. *Cyberpower and National Security*. Annapolis, MD: Potomac Books Inc, 2009.
Kuhn, Thomas. *The Structure of Scientific Revolutions*. Chicago, IL: The University of Chicago Press, 1996.

Lambeth, Benjamin S. *NATO's Air War For Kosovo: A Strategic and Operational Assessment*. Annapolis, MD: Rand Corporation, 2001.
Lambeth, Benjamin S. *The Transformation of American Air Power*. Annapolis, MD: Cornell University Press, 2000.
Libicki, Martin C. *Conquest in Cyberspace: National Security and Information Warfare*. Annapolis, MD: Cambridge University Press, 2007.
Lonsdale, David J. *The Nature of War in the Information Age: Clausewitzian Future (Strategy and History)*. Annapolis, MD: Routledge, 2004.
Mahan, Alfred Thayer. *Classics of Sea Power: Selections from the Writings of Rear Admiral Alfred Thayer Mahan.* Annapolis, MD: Naval Institute Press, 1991.
McDougall, Walter A. *. . . The Heavens and the Earth.* Baltimore, MD: Johns Hopkins University Press, 1997.
Moltz, James Clay. *The Politics of Space Security: Strategic Restraint and the Pursuit of National Interests*. Baltimore, MD: Stanford Security Studies, 2008.
Nye, Joseph S. *The Future of Power*. Baltimore, MD: PublicAffairs, 2011.
Ratcliff, R. A. *Delusions of Intelligence: Enigma, Ultra and the End of Secure Ciphers*. Annapolis, MD: Cambridge University Press, 2006.
Sheehan, Michael. *The International Politics of Space*. Baltimore, MD: Routledge, 2007.
Sheldon, John B. and Colin S. Gray, "Theory Ascendant? Spacepower and the Challenge of Strategic Theory" in *Toward a Theory of Spacepower: Selected Essays*, ed. Charles D. Lutes, et al., Washington, D.C.: National Defense University Press, 2011.
Singer, P.W. *Wired for War: The Robotics Revolution and Conflict in the 21st Century.* New York, NY: Penguin Books, 2009.

Briefings/Point Papers/Memos/Messages

"24th Air Force Mission Brief", October 31, 2011. E-mailed to author.
Brodeur, Lt Col Scott, 614 AOC Deputy Chief, Combat Operations Division, "JSpOC Overview Briefing." Briefing to author, February 21, 2012.
Brodeur, Lt Col Scott, 614 AOC Deputy Chief, Combat Operations Division, "JSpOC WIC Briefing." Briefing to author, February 21, 2012.
Fires Meeting. USCYBERCOM, February 23-24, 2012.
Moss, Col J. Christopher, JSpOC Commander, "JSpOC Road Show Briefing for SAASS." Briefing to SAASS Class XXI, April 18, 2012.

Secretary of Defense Memorandum, *Establishment of a Subordinate Unified US Cyber Command Under US Strategic Command for Military Cyberspace Operations*, June 23, 2009.
Secretary of Defense Memorandum, *Memorandum of Agreement Between The Department of Homeland Security and the Department of Defense Regarding Cybersecurity*, October 13, 2010.

Government Documents

24th Air Force Fact Sheet. http://www.24af.af.mil/library/factsheets/factsheet.asp?id=15663 (accessed on January 29, 2012).
Air Force Doctrine Document 2. *Operations and Organization,* April 3, 2007.
Air Force Doctrine Document 2-1.9. *Targeting*, June 8, 2006.
Air Force Doctrine Document 3-12. *Cyberspace Operations,* July 15 2010.
Air Force Doctrine Document 3-14. *Space Operations,* November 27, 2006 (incorporating Change 1, July 28, 2011).
Air Force Doctrine Document 6-0. *Command and Control*, June 1, 2007 (incorporating Change 1, July 28, 2011).
Air Force Instruction 13-1AOC, Volume 3. *Operational Procedures – Air and Space Operations Center,* November 2, 2011.
Air Force Tactics, Techniques, and Procedures 3-3.AOC. *Operational Employment – Air and Space Operations Center*, November 1, 2007.
Comprehensive National Cybersecurity Initiative, 2010. http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative.
Joint Publication 1. *Doctrine for the Armed Forces of the United States*, May 2, 2007 (incorporating Change 1, March 20, 2009).
Joint Publication 0-2. *Unified Action Armed Forces*, July 10, 2001.
Joint Publication 1-0. *Joint Personnel Support*, October 24, 2011.
Joint Publication 1-02. *Department of Defense Dictionary of Military and Associated Terms*, November 8, 2010 (updated October 15, 2011).
Joint Publication 3-30. *Command and Control of Joint Air Operations*, January 12, 2010.
JSpOC Fact Sheet. www.vandenberg.af.mil/library/factsheets (accessed on January 5, 2012).
United States Code. http://uscode.house.gov/ (accessed May 12, 2012).
USCYBERCOM Fact Sheet. www.stratcom.mil/factsheets/Cyber_Command/ (accessed on February 19, 2012).
USSTRATCOM Fact Sheet. http://www.stratcom.mil/functional_components/ (accessed on February 16, 2012).

Personal Communications – Interviews/E-Mails

Bayne, Capt Clara (24 AF/ACCE) in discussion with author, February 14, 21 & 23 and March 19, 2012.

Bixler, Maj Adam (24 AF/ACCE) in discussion with author, February 24 & March 29, 2012.

Brodeur, Lt Col Scott D. (614 AOC Deputy Chief, Combat Operations Division) in discussion with author, February 21, 2012.

Hatley, Lt Col Thomas (B-2 Pilot) in discussion with author, December 12, 2011.

Hathaway, Col David C. (24 AF/A3/5) in discussion with author, April 18, 2012.

Morris, Col Robert A. (24 AF/ACCE) in discussion with author, February 24, 2012.

Roy, Maj Francois (SAASS Student and CAOC NRO Liaison/ISR Element Chief during OIF/OEF) in discussion with author, January 10, 2012.

Smith, Col Michael V. (SAASS Instructor and MAAP Planner during OAF) in classroom discussion, February 7 & 10, 2012.

Sutton, Jason K. (AWC Student and previous Comm SQ/CC) in discussion with author on January, 17, 2012.

Reports

Department of Defense Cyberspace Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934. November 2011.

Department of Defense Quadrennial Defense Review. February 2010.

Department of Defense Strategy for Operating in Cyberspace. July 2011.

GAO-11-75, *Defense Department Cyber Efforts: DoD Faces Challenges in its Cyber Activities*. July 2011.

International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World. The White House. May 2011.

Lewis, James A. *Thresholds for Cyberwar*. Center for Strategic International Studies. Washington, D.C., September 2010.

National Military Strategy of the United States of America: Redefining America's Military Leadership. Joint Chiefs of Staff. 2011.

Sustaining US Global Leadership: Priorities for 21st Century Defense. Department of Defense. January 2012.

Speeches

Wynn, Michael W. "West Point Speech." Remarks at U.S. Military Academy, West Point, NY in Rebecca Grant "Victory in Cyberspace." *Air Force Association Special Report,* October 2006.